STRESS TEST DOCUMENT

High-Entropy Document Plate (Size Stress)

Image stress document 600 pages

CYBR-STRESS-101

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

Plate 1

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 1 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is evidenced by the quarterly review notes. The third-party register is reviewed against the approved design baseline. The third-party register is validated by the commissioning document. The remote access path is checked against the current written standard. Testing covers the failure case, not only the happy path.

Every internet-facing service is compared with the evidence pack held by the owner. The hardened build is traced to the commissioning document. The asset register is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The cloud baseline is validated by the evidence pack held by the owner. The encryption standard is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

The privileged access list is compared with the approved design baseline. The change process is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is checked against the quarterly review notes. The encryption standard is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

Plate 2

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 2 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is traced to the dependency map. The vendor register is documented alongside the commissioning document. The backup rotation is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

The change process is reconciled with the register of exceptions. The mobile standard is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is reviewed against the ticket history for the period. The classification scheme is evidenced by the agreed service level. The threat model is traced to the ticket history for the period. Every internet-facing service is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 3

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 3 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reconciled with the commissioning document. The classification scheme is reviewed against the ticket history for the period. The control is tested at least once every twelve months.

Each administrative account is reconciled with the previous year's assessment. Each administrative account is traced to the evidence pack held by the owner. The change process is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

The change process is measured against the signed exception log. The asset register is compared with the current written standard. The cloud baseline is evidenced by the previous year's assessment. The encryption standard is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The physical controls is evidenced by the current written standard. The continuity plan is documented alongside the register of exceptions. The vulnerability queue is evidenced by the signed exception log. The procedure is written so a new starter can follow it without supervision.

Plate 4

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 4 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is traced to the evidence pack held by the owner. The identity lifecycle is reviewed against the most recent exercise record. The identity lifecycle is documented alongside the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is reviewed against the previous year's assessment. The metric set is evidenced by the most recent exercise record. The encryption standard is compared with the commissioning document. Third parties must demonstrate the control before access is granted.

The hardened build is documented alongside the register of exceptions. The access review process is compared with the agreed service level. The privileged access list is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The hardened build is documented alongside the register of exceptions. The asset register is documented alongside the current written standard. The access review process is documented alongside the register of exceptions. The backup rotation is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

Plate 5

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 5 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is compared with the ticket history for the period. The vendor register is compared with the dependency map. Metrics are reported as trends rather than single data points.

The continuity plan is reviewed against the previous year's assessment. The backup rotation is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is traced to the ticket history for the period. The access review process is evidenced by the register of exceptions. The monitoring pipeline is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

Each administrative account is traced to the quarterly review notes. The asset register is checked against the agreed service level. The physical controls is traced to the current written standard. The cloud baseline is checked against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is documented alongside the approved design baseline. The recovery test is validated by the quarterly review notes. Any deviation requires written approval and an expiry date.

Plate 6

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 6 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is compared with the agreed service level. The physical controls is checked against the current written standard. The retention schedule is compared with the evidence pack held by the owner. The patch calendar is measured against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The physical controls is reconciled with the register of exceptions. The monitoring pipeline is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is checked against the approved design baseline. The metric set is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the most recent exercise record. The retention schedule is validated by the previous year's assessment. The monitoring pipeline is checked against the most recent exercise record. The risk register is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 7

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 7 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is traced to the dependency map. The remote access path is reviewed against the approved design baseline. The endpoint baseline is documented alongside the register of exceptions. Third parties must demonstrate the control before access is granted.

The risk register is evidenced by the dependency map. The remote access path is checked against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The risk register is measured against the register of exceptions. The asset register is evidenced by the evidence pack held by the owner. The asset register is evidenced by the current written standard. The encryption standard is measured against the commissioning document. The control is tested at least once every twelve months.

1. The encryption standard

The third-party register is traced to the ticket history for the period. The hardened build is documented alongside the signed exception log. The retention schedule is measured against the current written standard. The backup rotation is compared with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

Plate 8

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 8 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is reviewed against the register of exceptions. The vendor register is reconciled with the dependency map. The mobile standard is compared with the ticket history for the period. The privileged access list is reconciled with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

2. The patch calendar

The classification scheme is validated by the signed exception log. The endpoint baseline is checked against the approved design baseline. The third-party register is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is traced to the quarterly review notes. The awareness cycle is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the commissioning document. The change process is compared with the agreed service level. The segmentation boundary is reconciled with the evidence pack held by the owner. The hardened build is evidenced by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

Plate 9

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 9 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is compared with the commissioning document. The patch calendar is documented alongside the agreed service level. Testing covers the failure case, not only the happy path.

The risk register is measured against the dependency map. The patch calendar is reviewed against the quarterly review notes. The retention schedule is checked against the previous year's assessment. Any deviation requires written approval and an expiry date.

The retention schedule is reconciled with the commissioning document. The remote access path is checked against the approved design baseline. The metric set is validated by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is measured against the current written standard. The asset register is documented alongside the quarterly review notes. The segmentation boundary is documented alongside the approved design baseline. The retention schedule is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

The vendor register is compared with the agreed service level. The privileged access list is reconciled with the dependency map. The recovery test is checked against the previous year's assessment. Third parties must demonstrate the control before access is granted.

Plate 10

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 10 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is evidenced by the register of exceptions. The asset register is measured against the signed exception log. The privileged access list is measured against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is documented alongside the dependency map. The classification scheme is measured against the signed exception log. The remote access path is documented alongside the quarterly review notes. Any deviation requires written approval and an expiry date.

The asset register is compared with the quarterly review notes. The privileged access list is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is traced to the dependency map. The risk register is evidenced by the current written standard. The email authentication record is measured against the current written standard. The physical controls is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

Plate 11

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 11 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is checked against the approved design baseline. The email authentication record is evidenced by the ticket history for the period. The physical controls is compared with the agreed service level. The email authentication record is compared with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is documented alongside the evidence pack held by the owner. The hardened build is checked against the evidence pack held by the owner. The patch calendar is validated by the current written standard. The third-party register is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

The backup rotation is reconciled with the previous year's assessment. The remote access path is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The risk register is reconciled with the current written standard. The recovery test is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The email authentication record is documented alongside the current written standard. The continuity plan is measured against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 12

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 12 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is evidenced by the ticket history for the period. The email authentication record is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

4. The change process

The hardened build is reviewed against the approved design baseline. The patch calendar is evidenced by the commissioning document. The remote access path is reconciled with the ticket history for the period. The vulnerability queue is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The access review process is compared with the register of exceptions. The identity lifecycle is reconciled with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is compared with the commissioning document. The metric set is validated by the ticket history for the period. The recovery test is documented alongside the dependency map. The third-party register is checked against the dependency map. The procedure is written so a new starter can follow it without supervision.

Plate 13

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 13 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is validated by the quarterly review notes. The retention schedule is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

Each administrative account is evidenced by the agreed service level. The physical controls is measured against the approved design baseline. Every internet-facing service is documented alongside the current written standard. Every internet-facing service is reviewed against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is reviewed against the approved design baseline. The cloud baseline is measured against the register of exceptions. The intent is to make the safe path the default rather than an exception.

5. The encryption standard

The backup rotation is reviewed against the approved design baseline. The threat model is checked against the commissioning document. The third-party register is validated by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

Plate 14

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 14 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is traced to the register of exceptions. The email authentication record is traced to the most recent exercise record. The awareness cycle is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The remote access path is documented alongside the commissioning document. The classification scheme is validated by the most recent exercise record. The change process is compared with the commissioning document. The monitoring pipeline is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The metric set is traced to the quarterly review notes. The cloud baseline is traced to the most recent exercise record. The threat model is documented alongside the approved design baseline. Third parties must demonstrate the control before access is granted.

The privileged access list is evidenced by the ticket history for the period. The encryption standard is checked against the agreed service level. Each administrative account is measured against the approved design baseline. The monitoring pipeline is checked against the most recent exercise record. Third parties must demonstrate the control before access is granted.

Plate 15

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 15 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is compared with the quarterly review notes. The email authentication record is reviewed against the register of exceptions. The change process is evidenced by the current written standard. The segmentation boundary is reconciled with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The hardened build is evidenced by the approved design baseline. The risk register is evidenced by the previous year's assessment. The awareness cycle is documented alongside the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is traced to the evidence pack held by the owner. The classification scheme is validated by the current written standard. The change process is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The endpoint baseline is measured against the register of exceptions. The change process is traced to the agreed service level. The encryption standard is measured against the current written standard. The backup rotation is compared with the current written standard. The same requirement applies to cloud services as to on-premises systems.

Plate 16

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 16 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is evidenced by the previous year's assessment. The vendor register is evidenced by the register of exceptions. The privileged access list is compared with the dependency map. Records are retained only as long as the schedule requires.

The recovery test is measured against the dependency map. The backup rotation is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Acceptance criteria written before work starts.
- Test result attached to the record.
- Evidence stored in the shared evidence pack.

The segmentation boundary is validated by the quarterly review notes. The backup rotation is evidenced by the commissioning document. The access review process is validated by the previous year's assessment. The asset register is reviewed against the quarterly review notes. Any deviation requires written approval and an expiry date.

The risk register is validated by the signed exception log. The threat model is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

Plate 17

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 17 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is measured against the most recent exercise record. The vendor register is traced to the quarterly review notes. The continuity plan is checked against the register of exceptions. The physical controls is documented alongside the register of exceptions. Testing covers the failure case, not only the happy path.

The patch calendar is reviewed against the quarterly review notes. The email authentication record is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The hardened build is traced to the most recent exercise record. The patch calendar is reconciled with the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The continuity plan is validated by the agreed service level. The recovery test is checked against the current written standard. The control is tested at least once every twelve months.

The recovery test is validated by the current written standard. The asset register is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 18

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 18 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is compared with the agreed service level. The vendor register is checked against the signed exception log. Every internet-facing service is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The remote access path is measured against the evidence pack held by the owner. The identity lifecycle is checked against the dependency map. The endpoint baseline is measured against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is validated by the dependency map. The threat model is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is reconciled with the previous year's assessment. The mobile standard is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The threat model is evidenced by the most recent exercise record. The third-party register is reviewed against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 19

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 19 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is validated by the register of exceptions. The patch calendar is documented alongside the agreed service level. The metric set is compared with the most recent exercise record. The third-party register is validated by the signed exception log. The control is tested at least once every twelve months.

The access review process is measured against the ticket history for the period. The cloud baseline is documented alongside the ticket history for the period. The identity lifecycle is checked against the evidence pack held by the owner. The risk register is documented alongside the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The third-party register is compared with the register of exceptions. The retention schedule is checked against the agreed service level. The risk register is evidenced by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

6. The vendor register

Plate 20

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 20 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is documented alongside the previous year's assessment. Every internet-facing service is evidenced by the signed exception log. The backup rotation is compared with the agreed service level. The patch calendar is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is traced to the evidence pack held by the owner. The hardened build is reviewed against the dependency map. The third-party register is measured against the agreed service level. Records are retained only as long as the schedule requires.

The awareness cycle is compared with the quarterly review notes. Each administrative account is reconciled with the commissioning document. The vulnerability queue is evidenced by the evidence pack held by the owner. The classification scheme is traced to the approved design baseline. The control is tested at least once every twelve months.

The physical controls is reviewed against the ticket history for the period. The encryption standard is reviewed against the signed exception log. The physical controls is reconciled with the commissioning document. Testing covers the failure case, not only the happy path.

Plate 21

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 21 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is documented alongside the approved design baseline. The metric set is reviewed against the most recent exercise record. Every internet-facing service is validated by the current written standard. The identity lifecycle is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is measured against the ticket history for the period. The remote access path is reconciled with the current written standard. The awareness cycle is validated by the signed exception log. The identity lifecycle is traced to the quarterly review notes. Third parties must demonstrate the control before access is granted.

The remote access path is traced to the current written standard. The recovery test is measured against the current written standard. Every internet-facing service is evidenced by the commissioning document. Each administrative account is traced to the register of exceptions. Testing covers the failure case, not only the happy path.

Plate 22

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 22 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is compared with the quarterly review notes. The identity lifecycle is checked against the previous year's assessment. The identity lifecycle is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is reconciled with the quarterly review notes. The awareness cycle is documented alongside the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is checked against the agreed service level. The continuity plan is checked against the commissioning document. The cloud baseline is evidenced by the previous year's assessment. The encryption standard is compared with the approved design baseline. The control is tested at least once every twelve months.

The cloud baseline is traced to the dependency map. The change process is evidenced by the approved design baseline. The retention schedule is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

Plate 23

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 23 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is checked against the register of exceptions. The access review process is measured against the dependency map. The access review process is reconciled with the dependency map. The control is tested at least once every twelve months.

The monitoring pipeline is traced to the quarterly review notes. Each administrative account is reconciled with the signed exception log. The cloud baseline is documented alongside the most recent exercise record. The control is tested at least once every twelve months.

The third-party register is reconciled with the most recent exercise record. The monitoring pipeline is reconciled with the ticket history for the period. The hardened build is evidenced by the agreed service level. The recovery test is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.

Plate 24

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 24 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is traced to the approved design baseline. The endpoint baseline is measured against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is checked against the agreed service level. The metric set is reconciled with the agreed service level. The encryption standard is reviewed against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is reviewed against the signed exception log. The threat model is measured against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The classification scheme is compared with the evidence pack held by the owner. The retention schedule is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The awareness cycle is evidenced by the previous year's assessment. The threat model is reviewed against the most recent exercise record. The retention schedule is documented alongside the register of exceptions. Metrics are reported as trends rather than single data points.

Plate 25

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 25 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is checked against the previous year's assessment. The backup rotation is reviewed against the evidence pack held by the owner. The threat model is reviewed against the most recent exercise record. The access review process is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The hardened build is compared with the ticket history for the period. Every internet-facing service is documented alongside the commissioning document. The threat model is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The recovery test is measured against the most recent exercise record. The email authentication record is measured against the most recent exercise record. The endpoint baseline is traced to the previous year's assessment. The physical controls is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The classification scheme is compared with the previous year's assessment. The vulnerability queue is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Plate 26

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 26 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is reconciled with the register of exceptions. The retention schedule is evidenced by the agreed service level. The mobile standard is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is documented alongside the commissioning document. The monitoring pipeline is validated by the signed exception log. The vendor register is traced to the ticket history for the period. The backup rotation is validated by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is traced to the ticket history for the period. The risk register is traced to the evidence pack held by the owner. The continuity plan is compared with the dependency map. The continuity plan is traced to the approved design baseline. Third parties must demonstrate the control before access is granted.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

Plate 27

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 27 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is reviewed against the previous year's assessment. The metric set is compared with the evidence pack held by the owner. The risk register is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reviewed against the approved design baseline. The endpoint baseline is evidenced by the signed exception log. The hardened build is documented alongside the signed exception log. The threat model is reviewed against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The continuity plan is traced to the evidence pack held by the owner. The threat model is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

The mobile standard is traced to the signed exception log. The segmentation boundary is validated by the dependency map. The endpoint baseline is traced to the approved design baseline. Testing covers the failure case, not only the happy path.

The monitoring pipeline is compared with the commissioning document. The backup rotation is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Plate 28

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 28 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is measured against the previous year's assessment. The recovery test is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The recovery test is traced to the register of exceptions. The vulnerability queue is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

Every internet-facing service is reconciled with the evidence pack held by the owner. The threat model is measured against the previous year's assessment. The remote access path is evidenced by the current written standard. The endpoint baseline is checked against the agreed service level. The control is tested at least once every twelve months.

The change process is reviewed against the most recent exercise record. The monitoring pipeline is traced to the dependency map. The endpoint baseline is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The access review process is evidenced by the most recent exercise record. The hardened build is reconciled with the evidence pack held by the owner. The monitoring pipeline is reconciled with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Plate 29

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 29 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is traced to the previous year's assessment. The classification scheme is evidenced by the approved design baseline. The privileged access list is compared with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is reviewed against the quarterly review notes. The classification scheme is measured against the current written standard. The physical controls is measured against the signed exception log. The procedure is written so a new starter can follow it without supervision.

7. The cloud baseline

The patch calendar is evidenced by the previous year's assessment. The metric set is documented alongside the dependency map. The continuity plan is compared with the current written standard. The change process is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is compared with the evidence pack held by the owner. The backup rotation is reconciled with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

Plate 30

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 30 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is evidenced by the ticket history for the period. The email authentication record is documented alongside the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is traced to the commissioning document. The monitoring pipeline is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is evidenced by the ticket history for the period. The email authentication record is measured against the agreed service level. The third-party register is reviewed against the register of exceptions. Any deviation requires written approval and an expiry date.

The access review process is reviewed against the signed exception log. The privileged access list is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is evidenced by the previous year's assessment. The risk register is validated by the dependency map. The risk register is evidenced by the agreed service level. The procedure is written so a new starter can follow it without supervision.

Plate 31

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 31 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is traced to the agreed service level. Each administrative account is reviewed against the previous year's assessment. The risk register is reviewed against the agreed service level. The awareness cycle is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The recovery test is compared with the quarterly review notes. The awareness cycle is checked against the previous year's assessment. The patch calendar is measured against the previous year's assessment. The control is tested at least once every twelve months.

The classification scheme is reviewed against the current written standard. The metric set is documented alongside the previous year's assessment. The third-party register is evidenced by the most recent exercise record. The retention schedule is reviewed against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Plate 32

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 32 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is validated by the most recent exercise record. The physical controls is traced to the commissioning document. The asset register is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The metric set is measured against the previous year's assessment. The risk register is evidenced by the approved design baseline. The change process is traced to the evidence pack held by the owner. The segmentation boundary is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is reviewed against the ticket history for the period. The asset register is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is measured against the commissioning document. The privileged access list is reviewed against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is reviewed against the evidence pack held by the owner. Each administrative account is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

Plate 33

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 33 - 232 x 232 px, DeviceRGB, FlateDecode

8. The third-party register

The mobile standard is validated by the previous year's assessment. The cloud baseline is documented alongside the register of exceptions. The identity lifecycle is validated by the commissioning document. Every internet-facing service is documented alongside the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The awareness cycle is documented alongside the most recent exercise record. The change process is reviewed against the commissioning document. The retention schedule is reviewed against the ticket history for the period. The vendor register is measured against the approved design baseline. Third parties must demonstrate the control before access is granted.

The threat model is validated by the most recent exercise record. The third-party register is checked against the register of exceptions. The awareness cycle is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is evidenced by the agreed service level. Every internet-facing service is reconciled with the commissioning document. The encryption standard is reviewed against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 34

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 34 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is traced to the quarterly review notes. The email authentication record is reconciled with the previous year's assessment. Metrics are reported as trends rather than single data points.

The mobile standard is evidenced by the agreed service level. The identity lifecycle is checked against the register of exceptions. Testing covers the failure case, not only the happy path.

The patch calendar is compared with the commissioning document. The encryption standard is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The remote access path is evidenced by the most recent exercise record. The vulnerability queue is measured against the dependency map. The threat model is validated by the dependency map. Third parties must demonstrate the control before access is granted.

The email authentication record is checked against the agreed service level. The risk register is reconciled with the agreed service level. The segmentation boundary is traced to the approved design baseline. The segmentation boundary is validated by the dependency map. Records are retained only as long as the schedule requires.

Plate 35

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 35 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is checked against the dependency map. The recovery test is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is reviewed against the quarterly review notes. The change process is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the evidence pack held by the owner. The endpoint baseline is reviewed against the register of exceptions. The privileged access list is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

- Exception route documented and time-bound.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.

Plate 36

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 36 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reviewed against the most recent exercise record. The mobile standard is compared with the approved design baseline. The classification scheme is reconciled with the most recent exercise record. The monitoring pipeline is evidenced by the agreed service level. The control is tested at least once every twelve months.

The mobile standard is checked against the current written standard. The mobile standard is measured against the signed exception log. The control is tested at least once every twelve months.

Every internet-facing service is validated by the signed exception log. The encryption standard is checked against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

9. The hardened build

The classification scheme is evidenced by the approved design baseline. The metric set is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 37

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 37 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is reviewed against the signed exception log. The vendor register is documented alongside the signed exception log. The monitoring pipeline is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The hardened build is measured against the most recent exercise record. The change process is documented alongside the current written standard. The continuity plan is documented alongside the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The retention schedule is reviewed against the ticket history for the period. The retention schedule is measured against the most recent exercise record. The endpoint baseline is measured against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is traced to the ticket history for the period. The remote access path is reconciled with the register of exceptions. Each administrative account is measured against the approved design baseline. The patch calendar is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Plate 38

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 38 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is evidenced by the approved design baseline. The mobile standard is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

Every internet-facing service is evidenced by the most recent exercise record. The identity lifecycle is documented alongside the dependency map. The mobile standard is reviewed against the ticket history for the period. The control is tested at least once every twelve months.

The backup rotation is compared with the previous year's assessment. The encryption standard is traced to the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is validated by the ticket history for the period. The cloud baseline is evidenced by the commissioning document. The vulnerability queue is reviewed against the signed exception log. The email authentication record is checked against the commissioning document. Metrics are reported as trends rather than single data points.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.

Plate 39

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 39 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is measured against the quarterly review notes. The encryption standard is evidenced by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is traced to the signed exception log. The monitoring pipeline is compared with the ticket history for the period. The continuity plan is evidenced by the commissioning document. The hardened build is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The remote access path is traced to the most recent exercise record. The classification scheme is reviewed against the approved design baseline. The vulnerability queue is reviewed against the ticket history for the period. The backup rotation is measured against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is measured against the approved design baseline. The risk register is compared with the current written standard. The segmentation boundary is documented alongside the quarterly review notes. The continuity plan is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

Plate 40

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 40 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is measured against the commissioning document. The retention schedule is reconciled with the previous year's assessment. The access review process is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is reconciled with the previous year's assessment. The vulnerability queue is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is evidenced by the evidence pack held by the owner. The change process is checked against the quarterly review notes. The monitoring pipeline is checked against the approved design baseline. The segmentation boundary is reviewed against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is traced to the most recent exercise record. The metric set is checked against the previous year's assessment. The third-party register is traced to the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is reconciled with the evidence pack held by the owner. The access review process is compared with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Plate 41

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 41 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is reviewed against the evidence pack held by the owner. The mobile standard is validated by the previous year's assessment. Any deviation requires written approval and an expiry date.

The email authentication record is documented alongside the approved design baseline. The identity lifecycle is checked against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The third-party register is documented alongside the most recent exercise record. The retention schedule is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is compared with the dependency map. The backup rotation is reviewed against the current written standard. The hardened build is measured against the previous year's assessment. The control is tested at least once every twelve months.

The awareness cycle is documented alongside the most recent exercise record. The cloud baseline is reconciled with the quarterly review notes. The endpoint baseline is compared with the register of exceptions. The vulnerability queue is reviewed against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

Plate 42

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 42 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is checked against the quarterly review notes. The patch calendar is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Test result attached to the record.
- Backup of the change retained for rollback.

The mobile standard is compared with the quarterly review notes. The backup rotation is validated by the dependency map. Any deviation requires written approval and an expiry date.

10. The patch calendar

The encryption standard is traced to the signed exception log. The endpoint baseline is reviewed against the signed exception log. The risk register is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is compared with the ticket history for the period. The encryption standard is evidenced by the current written standard. The endpoint baseline is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

Plate 43

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 43 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is reviewed against the current written standard. The encryption standard is reviewed against the approved design baseline. The threat model is documented alongside the current written standard. The metric set is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is reconciled with the approved design baseline. The vendor register is traced to the most recent exercise record. The threat model is validated by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is compared with the agreed service level. The metric set is documented alongside the dependency map. The risk register is compared with the most recent exercise record. The asset register is validated by the agreed service level. Any deviation requires written approval and an expiry date.

The patch calendar is reconciled with the commissioning document. The threat model is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

Plate 44

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 44 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is reconciled with the register of exceptions. The monitoring pipeline is reconciled with the previous year's assessment. The remote access path is evidenced by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is documented alongside the approved design baseline. The vendor register is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is evidenced by the commissioning document. The remote access path is traced to the quarterly review notes. The threat model is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

- Exception route documented and time-bound.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The continuity plan is checked against the previous year's assessment. The continuity plan is compared with the commissioning document. The monitoring pipeline is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

Plate 45

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 45 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reconciled with the approved design baseline. The email authentication record is compared with the current written standard. The hardened build is compared with the commissioning document. The recovery test is documented alongside the evidence pack held by the owner. The control is tested at least once every twelve months.

The awareness cycle is checked against the approved design baseline. The change process is measured against the previous year's assessment. The vulnerability queue is measured against the register of exceptions. The remote access path is traced to the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is checked against the agreed service level. The risk register is checked against the most recent exercise record. The monitoring pipeline is evidenced by the previous year's assessment. The classification scheme is documented alongside the agreed service level. Third parties must demonstrate the control before access is granted.

The awareness cycle is measured against the dependency map. The access review process is checked against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Plate 46

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 46 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is checked against the signed exception log. The identity lifecycle is compared with the most recent exercise record. The threat model is evidenced by the signed exception log. The segmentation boundary is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The hardened build is reviewed against the most recent exercise record. The retention schedule is validated by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is reviewed against the quarterly review notes. The awareness cycle is measured against the commissioning document. The remote access path is traced to the commissioning document. Every internet-facing service is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.

Plate 47

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 47 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is documented alongside the quarterly review notes. The monitoring pipeline is documented alongside the signed exception log. The physical controls is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is documented alongside the evidence pack held by the owner. The hardened build is checked against the register of exceptions. The access review process is reviewed against the commissioning document. The backup rotation is checked against the commissioning document. The intent is to make the safe path the default rather than an exception.

The asset register is reviewed against the most recent exercise record. The email authentication record is validated by the ticket history for the period. Each administrative account is checked against the evidence pack held by the owner. The cloud baseline is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The encryption standard is compared with the current written standard. The privileged access list is traced to the signed exception log. The change process is checked against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 48

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 48 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is traced to the evidence pack held by the owner. The hardened build is reviewed against the most recent exercise record. The privileged access list is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.

The classification scheme is reconciled with the previous year's assessment. The classification scheme is evidenced by the dependency map. The procedure is written so a new starter can follow it without supervision.

The patch calendar is evidenced by the quarterly review notes. The endpoint baseline is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

Plate 49

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 49 - 232 x 232 px, DeviceRGB, FlateDecode

11. The identity lifecycle

Each administrative account is measured against the current written standard. The metric set is checked against the quarterly review notes. The retention schedule is traced to the dependency map. The physical controls is validated by the ticket history for the period. The control is tested at least once every twelve months.

Every internet-facing service is evidenced by the previous year's assessment. The email authentication record is checked against the current written standard. The endpoint baseline is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is validated by the agreed service level. The mobile standard is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is checked against the evidence pack held by the owner. The mobile standard is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 50

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 50 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is measured against the most recent exercise record. The encryption standard is compared with the register of exceptions. The segmentation boundary is evidenced by the approved design baseline. The email authentication record is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The hardened build is reviewed against the agreed service level. Each administrative account is checked against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

12. The classification scheme

The privileged access list is documented alongside the dependency map. The privileged access list is reconciled with the evidence pack held by the owner. The endpoint baseline is validated by the most recent exercise record. The backup rotation is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

Plate 51

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 51 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is documented alongside the dependency map. The patch calendar is documented alongside the register of exceptions. The awareness cycle is measured against the commissioning document. The hardened build is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is validated by the evidence pack held by the owner. The physical controls is measured against the approved design baseline. The recovery test is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The asset register is documented alongside the most recent exercise record. The retention schedule is validated by the approved design baseline. The monitoring pipeline is compared with the previous year's assessment. The backup rotation is evidenced by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The change process is validated by the signed exception log. The metric set is compared with the agreed service level. Each administrative account is reviewed against the signed exception log. The change process is reviewed against the signed exception log. Records are retained only as long as the schedule requires.

Plate 52

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 52 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is compared with the quarterly review notes. The backup rotation is compared with the signed exception log. The backup rotation is documented alongside the register of exceptions. Each administrative account is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The asset register is compared with the dependency map. The recovery test is evidenced by the most recent exercise record. The vulnerability queue is evidenced by the approved design baseline. The endpoint baseline is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is compared with the approved design baseline. The identity lifecycle is reconciled with the previous year's assessment. The awareness cycle is measured against the ticket history for the period. The vendor register is traced to the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is reconciled with the ticket history for the period. The awareness cycle is validated by the evidence pack held by the owner. The segmentation boundary is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 53

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 53 - 232 x 232 px, DeviceRGB, FlateDecode

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Review date scheduled and visible.

The vulnerability queue is reviewed against the register of exceptions. The third-party register is measured against the approved design baseline. The mobile standard is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is compared with the previous year's assessment. The backup rotation is reconciled with the commissioning document. The recovery test is documented alongside the commissioning document. The remote access path is evidenced by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is traced to the quarterly review notes. The recovery test is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

Plate 54

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 54 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reviewed against the current written standard. The monitoring pipeline is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

The asset register is checked against the quarterly review notes. The cloud baseline is compared with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is reviewed against the quarterly review notes. The privileged access list is validated by the register of exceptions. The change process is traced to the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is reviewed against the approved design baseline. The access review process is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is reconciled with the dependency map. The awareness cycle is documented alongside the evidence pack held by the owner. The backup rotation is reconciled with the current written standard. The retention schedule is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 55

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 55 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is measured against the most recent exercise record. Every internet-facing service is evidenced by the evidence pack held by the owner. The continuity plan is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The change process is documented alongside the agreed service level. The third-party register is reviewed against the register of exceptions. The access review process is checked against the approved design baseline. The email authentication record is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is documented alongside the previous year's assessment. The patch calendar is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is reconciled with the commissioning document. Each administrative account is documented alongside the ticket history for the period. The email authentication record is reviewed against the ticket history for the period. The remote access path is checked against the register of exceptions. Third parties must demonstrate the control before access is granted.

Plate 56

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 56 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is traced to the agreed service level. The third-party register is traced to the quarterly review notes. The identity lifecycle is documented alongside the most recent exercise record. The vendor register is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is validated by the agreed service level. The identity lifecycle is evidenced by the most recent exercise record. The risk register is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is measured against the approved design baseline. The endpoint baseline is measured against the previous year's assessment. The recovery test is validated by the ticket history for the period. The backup rotation is evidenced by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The risk register is evidenced by the dependency map. The risk register is evidenced by the commissioning document. The threat model is measured against the evidence pack held by the owner. The threat model is checked against the dependency map. Any deviation requires written approval and an expiry date.

Plate 57

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 57 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is documented alongside the quarterly review notes. The third-party register is evidenced by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is validated by the dependency map. The retention schedule is traced to the most recent exercise record. The hardened build is evidenced by the evidence pack held by the owner. The patch calendar is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The privileged access list is reviewed against the quarterly review notes. The encryption standard is reconciled with the signed exception log. The continuity plan is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reconciled with the current written standard. The vulnerability queue is evidenced by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is measured against the dependency map. The segmentation boundary is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Plate 58

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 58 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is reviewed against the register of exceptions. The awareness cycle is checked against the approved design baseline. The access review process is checked against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is validated by the approved design baseline. The identity lifecycle is reconciled with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is reviewed against the most recent exercise record. The cloud baseline is validated by the dependency map. The identity lifecycle is compared with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

13. The metric set

The metric set is reviewed against the most recent exercise record. The mobile standard is measured against the agreed service level. The segmentation boundary is compared with the previous year's assessment. Every internet-facing service is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vendor register is checked against the agreed service level. The threat model is reconciled with the previous year's assessment. Metrics are reported as trends rather than single data points.

Plate 59

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 59 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is reconciled with the signed exception log. The vendor register is checked against the agreed service level. The endpoint baseline is compared with the agreed service level. The risk register is checked against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is compared with the evidence pack held by the owner. The cloud baseline is validated by the quarterly review notes. The access review process is measured against the quarterly review notes. Metrics are reported as trends rather than single data points.

The patch calendar is measured against the register of exceptions. The backup rotation is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The email authentication record is evidenced by the ticket history for the period. The risk register is reconciled with the previous year's assessment. Every internet-facing service is measured against the evidence pack held by the owner. The retention schedule is reviewed against the agreed service level. The control is tested at least once every twelve months.

The metric set is reconciled with the ticket history for the period. The hardened build is checked against the evidence pack held by the owner. The risk register is compared with the current written standard. Metrics are reported as trends rather than single data points.

Plate 60

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 60 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is documented alongside the commissioning document. The encryption standard is compared with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is evidenced by the ticket history for the period. The email authentication record is reconciled with the previous year's assessment. The mobile standard is reviewed against the commissioning document. Third parties must demonstrate the control before access is granted.

14. The classification scheme

The retention schedule is measured against the previous year's assessment. The patch calendar is validated by the current written standard. The threat model is reviewed against the previous year's assessment. The vendor register is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The continuity plan is checked against the most recent exercise record. The recovery test is evidenced by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

Plate 61

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 61 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is traced to the dependency map. The backup rotation is reviewed against the most recent exercise record. The retention schedule is reviewed against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The third-party register is documented alongside the signed exception log. The vendor register is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is traced to the most recent exercise record. The monitoring pipeline is evidenced by the ticket history for the period. The threat model is validated by the ticket history for the period. The email authentication record is reviewed against the approved design baseline. Third parties must demonstrate the control before access is granted.

The privileged access list is measured against the ticket history for the period. The email authentication record is evidenced by the signed exception log. The asset register is compared with the approved design baseline. The access review process is compared with the current written standard. Where automation is possible, the manual step is retained as a fallback.

Plate 62

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 62 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is documented alongside the current written standard. The mobile standard is evidenced by the most recent exercise record. The change process is documented alongside the register of exceptions. The change process is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The patch calendar is measured against the commissioning document. The continuity plan is checked against the register of exceptions. Metrics are reported as trends rather than single data points.

Each administrative account is compared with the current written standard. The encryption standard is documented alongside the agreed service level. The awareness cycle is reviewed against the current written standard. The privileged access list is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is evidenced by the ticket history for the period. The patch calendar is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is traced to the register of exceptions. The backup rotation is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

Plate 63

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 63 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is evidenced by the approved design baseline. The patch calendar is reconciled with the ticket history for the period. The vulnerability queue is checked against the agreed service level. The risk register is evidenced by the signed exception log. Any deviation requires written approval and an expiry date.

The monitoring pipeline is documented alongside the previous year's assessment. The classification scheme is reviewed against the ticket history for the period. The segmentation boundary is traced to the signed exception log. The privileged access list is measured against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is evidenced by the register of exceptions. Each administrative account is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The awareness cycle is documented alongside the signed exception log. The remote access path is validated by the register of exceptions. The email authentication record is validated by the register of exceptions. The awareness cycle is checked against the dependency map. The intent is to make the safe path the default rather than an exception.

Plate 64

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 64 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is evidenced by the quarterly review notes. The threat model is measured against the agreed service level. The intent is to make the safe path the default rather than an exception.

The continuity plan is validated by the register of exceptions. The encryption standard is checked against the register of exceptions. The vendor register is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is validated by the register of exceptions. The endpoint baseline is documented alongside the register of exceptions. The privileged access list is evidenced by the previous year's assessment. The retention schedule is measured against the agreed service level. Third parties must demonstrate the control before access is granted.

The physical controls is checked against the quarterly review notes. The encryption standard is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The third-party register is reconciled with the dependency map. The patch calendar is documented alongside the evidence pack held by the owner. The cloud baseline is evidenced by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

Plate 65

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 65 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is validated by the current written standard. The recovery test is traced to the evidence pack held by the owner. The threat model is validated by the previous year's assessment. Testing covers the failure case, not only the happy path.

The mobile standard is measured against the commissioning document. The continuity plan is reviewed against the agreed service level. The threat model is validated by the evidence pack held by the owner. The vulnerability queue is documented alongside the signed exception log. Third parties must demonstrate the control before access is granted.

The metric set is checked against the most recent exercise record. The email authentication record is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The metric set is evidenced by the commissioning document. The access review process is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is documented alongside the dependency map. The backup rotation is validated by the signed exception log. The recovery test is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 66

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 66 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is traced to the current written standard. The vendor register is reconciled with the commissioning document. The vulnerability queue is documented alongside the ticket history for the period. The encryption standard is evidenced by the most recent exercise record. Testing covers the failure case, not only the happy path.

The endpoint baseline is validated by the signed exception log. The classification scheme is traced to the most recent exercise record. Each administrative account is measured against the current written standard. The risk register is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is documented alongside the commissioning document. The asset register is evidenced by the previous year's assessment. The segmentation boundary is reviewed against the current written standard. The control is tested at least once every twelve months.

The email authentication record is validated by the signed exception log. The vendor register is reviewed against the most recent exercise record. The metric set is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

Plate 67

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 67 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is evidenced by the commissioning document. The hardened build is checked against the commissioning document. The email authentication record is reviewed against the ticket history for the period. The backup rotation is documented alongside the agreed service level. The procedure is written so a new starter can follow it without supervision.

The risk register is evidenced by the ticket history for the period. The hardened build is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is measured against the ticket history for the period. The change process is validated by the quarterly review notes. The access review process is documented alongside the previous year's assessment. Third parties must demonstrate the control before access is granted.

The hardened build is reconciled with the evidence pack held by the owner. The patch calendar is reconciled with the quarterly review notes. The backup rotation is validated by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is documented alongside the most recent exercise record. The change process is reconciled with the signed exception log. The endpoint baseline is reconciled with the current written standard. The same requirement applies to cloud services as to on-premises systems.

Plate 68

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 68 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is reconciled with the evidence pack held by the owner. The endpoint baseline is checked against the approved design baseline. The email authentication record is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is traced to the evidence pack held by the owner. The change process is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The vendor register is documented alongside the register of exceptions. The segmentation boundary is reviewed against the dependency map. The segmentation boundary is compared with the previous year's assessment. The continuity plan is reviewed against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is evidenced by the current written standard. The backup rotation is compared with the dependency map. The patch calendar is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is traced to the most recent exercise record. The hardened build is checked against the quarterly review notes. The metric set is documented alongside the evidence pack held by the owner. The third-party register is documented alongside the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 69

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 69 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is reviewed against the register of exceptions. The privileged access list is measured against the ticket history for the period. The change process is measured against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is validated by the previous year's assessment. The patch calendar is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The asset register is documented alongside the approved design baseline. Each administrative account is measured against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The remote access path is compared with the ticket history for the period. Every internet-facing service is traced to the signed exception log. The mobile standard is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The classification scheme is evidenced by the previous year's assessment. The change process is checked against the previous year's assessment. The cloud baseline is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Plate 70

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 70 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is validated by the signed exception log. The segmentation boundary is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

- Test result attached to the record.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Review date scheduled and visible.

The identity lifecycle is traced to the current written standard. The vendor register is evidenced by the register of exceptions. The physical controls is evidenced by the current written standard. The segmentation boundary is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is traced to the approved design baseline. The backup rotation is reviewed against the signed exception log. Any deviation requires written approval and an expiry date.

Every internet-facing service is evidenced by the dependency map. The retention schedule is validated by the ticket history for the period. The cloud baseline is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Plate 71

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 71 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is compared with the signed exception log. The recovery test is reconciled with the agreed service level. Each administrative account is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

15. Each administrative account

The hardened build is reconciled with the ticket history for the period. Each administrative account is checked against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

16. The continuity plan

Every internet-facing service is checked against the quarterly review notes. The continuity plan is traced to the current written standard. The email authentication record is reviewed against the commissioning document. The hardened build is checked against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 72

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 72 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is reconciled with the signed exception log. The physical controls is validated by the most recent exercise record. The vulnerability queue is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The retention schedule is evidenced by the evidence pack held by the owner. The backup rotation is validated by the register of exceptions. The continuity plan is traced to the approved design baseline. The vendor register is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is validated by the current written standard. The asset register is reviewed against the current written standard. The change process is traced to the quarterly review notes. The identity lifecycle is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

The vendor register is evidenced by the previous year's assessment. The backup rotation is documented alongside the register of exceptions. The endpoint baseline is evidenced by the dependency map. Third parties must demonstrate the control before access is granted.

Plate 73

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 73 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is evidenced by the signed exception log. The remote access path is checked against the commissioning document. The risk register is checked against the commissioning document. The third-party register is documented alongside the register of exceptions. Records are retained only as long as the schedule requires.

The backup rotation is evidenced by the most recent exercise record. The backup rotation is compared with the current written standard. The intent is to make the safe path the default rather than an exception.

The asset register is checked against the most recent exercise record. The monitoring pipeline is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is validated by the agreed service level. The risk register is compared with the current written standard. The email authentication record is checked against the commissioning document. The segmentation boundary is documented alongside the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

Plate 74

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 74 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reconciled with the most recent exercise record. The recovery test is evidenced by the previous year's assessment. The encryption standard is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The continuity plan is compared with the dependency map. The encryption standard is validated by the most recent exercise record. The metric set is reviewed against the commissioning document. The hardened build is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The email authentication record is checked against the evidence pack held by the owner. The classification scheme is traced to the ticket history for the period. The vulnerability queue is traced to the previous year's assessment. The recovery test is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is reconciled with the most recent exercise record. The retention schedule is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 75

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 75 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is reconciled with the evidence pack held by the owner. The threat model is reconciled with the dependency map. The access review process is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is reconciled with the signed exception log. Each administrative account is reviewed against the ticket history for the period. Records are retained only as long as the schedule requires.

The awareness cycle is measured against the current written standard. The patch calendar is reviewed against the commissioning document. The patch calendar is documented alongside the ticket history for the period. The classification scheme is compared with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is evidenced by the commissioning document. The change process is evidenced by the previous year's assessment. The hardened build is traced to the agreed service level. The monitoring pipeline is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Plate 76

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 76 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is documented alongside the evidence pack held by the owner. The asset register is validated by the commissioning document. The risk register is evidenced by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The vendor register is compared with the commissioning document. The metric set is measured against the quarterly review notes. The continuity plan is documented alongside the approved design baseline. The metric set is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

17. The cloud baseline

The patch calendar is documented alongside the register of exceptions. The privileged access list is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

18. The hardened build

Plate 77

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 77 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is traced to the signed exception log. The third-party register is reconciled with the ticket history for the period. The vendor register is compared with the most recent exercise record. The retention schedule is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is reconciled with the signed exception log. The encryption standard is traced to the quarterly review notes. The hardened build is measured against the signed exception log. Testing covers the failure case, not only the happy path.

The mobile standard is documented alongside the ticket history for the period. The email authentication record is traced to the ticket history for the period. The asset register is traced to the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The hardened build is measured against the dependency map. The recovery test is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The threat model is validated by the quarterly review notes. The vulnerability queue is measured against the commissioning document. The third-party register is validated by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

Plate 78

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 78 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is measured against the quarterly review notes. Every internet-facing service is checked against the current written standard. The backup rotation is reconciled with the current written standard. The change process is checked against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The vendor register is traced to the agreed service level. The physical controls is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The email authentication record is measured against the signed exception log. The metric set is reviewed against the previous year's assessment. The threat model is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The encryption standard is validated by the ticket history for the period. The recovery test is traced to the approved design baseline. The metric set is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is traced to the agreed service level. The privileged access list is reviewed against the evidence pack held by the owner. The threat model is traced to the approved design baseline. The awareness cycle is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Plate 79

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 79 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is documented alongside the evidence pack held by the owner. The classification scheme is traced to the register of exceptions. The retention schedule is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The remote access path is compared with the approved design baseline. The patch calendar is compared with the quarterly review notes. The access review process is measured against the register of exceptions. The recovery test is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

The patch calendar is compared with the approved design baseline. The backup rotation is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The awareness cycle is reviewed against the register of exceptions. The continuity plan is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Plate 80

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 80 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is traced to the current written standard. The third-party register is checked against the ticket history for the period. The monitoring pipeline is evidenced by the current written standard. The encryption standard is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The physical controls is traced to the current written standard. The segmentation boundary is measured against the approved design baseline. The threat model is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The recovery test is traced to the dependency map. The encryption standard is reconciled with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reconciled with the dependency map. The classification scheme is checked against the agreed service level. The vulnerability queue is evidenced by the agreed service level. The control is tested at least once every twelve months.

Plate 81

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 81 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is measured against the previous year's assessment. The threat model is measured against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is validated by the dependency map. The segmentation boundary is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

20. The email authentication record

The asset register is measured against the evidence pack held by the owner. The privileged access list is traced to the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is documented alongside the dependency map. The awareness cycle is checked against the previous year's assessment. The physical controls is validated by the most recent exercise record. Metrics are reported as trends rather than single data points.

The hardened build is reviewed against the signed exception log. The access review process is checked against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 82

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 82 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is reviewed against the register of exceptions. The classification scheme is compared with the commissioning document. The metric set is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is compared with the quarterly review notes. The mobile standard is traced to the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is compared with the ticket history for the period. The threat model is evidenced by the agreed service level. The control is tested at least once every twelve months.

The classification scheme is traced to the dependency map. The encryption standard is checked against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is reconciled with the agreed service level. Each administrative account is reconciled with the approved design baseline. The continuity plan is measured against the approved design baseline. The intent is to make the safe path the default rather than an exception.

Plate 83

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 83 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is checked against the signed exception log. The physical controls is reconciled with the dependency map. The email authentication record is checked against the ticket history for the period. The backup rotation is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The remote access path is traced to the previous year's assessment. The physical controls is checked against the signed exception log. The vendor register is traced to the agreed service level. Third parties must demonstrate the control before access is granted.

The continuity plan is traced to the commissioning document. The access review process is evidenced by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is compared with the quarterly review notes. The access review process is reviewed against the quarterly review notes. The privileged access list is reviewed against the register of exceptions. The hardened build is checked against the commissioning document. Testing covers the failure case, not only the happy path.

Plate 84

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 84 - 232 x 232 px, DeviceRGB, FlateDecode

21. Every internet-facing service

The email authentication record is checked against the register of exceptions. The hardened build is traced to the commissioning document. The remote access path is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is compared with the dependency map. The endpoint baseline is traced to the commissioning document. The third-party register is reviewed against the current written standard. The mobile standard is reviewed against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

The third-party register is validated by the previous year's assessment. The backup rotation is compared with the signed exception log. The continuity plan is compared with the register of exceptions. The email authentication record is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

Plate 85

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 85 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is evidenced by the register of exceptions. The email authentication record is reviewed against the evidence pack held by the owner. The vendor register is validated by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is documented alongside the register of exceptions. The third-party register is reconciled with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is validated by the most recent exercise record. The email authentication record is validated by the commissioning document. The hardened build is checked against the most recent exercise record. The asset register is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is reviewed against the quarterly review notes. The classification scheme is traced to the commissioning document. Any deviation requires written approval and an expiry date.

The metric set is traced to the previous year's assessment. The cloud baseline is compared with the most recent exercise record. The patch calendar is checked against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Plate 86

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 86 - 232 x 232 px, DeviceRGB, FlateDecode

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Review date scheduled and visible.

23. The encryption standard

The awareness cycle is validated by the previous year's assessment. The hardened build is compared with the previous year's assessment. The third-party register is traced to the current written standard. Testing covers the failure case, not only the happy path.

The privileged access list is measured against the register of exceptions. The remote access path is reconciled with the quarterly review notes. The hardened build is measured against the ticket history for the period. The third-party register is measured against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

24. The vendor register

The physical controls is checked against the agreed service level. The physical controls is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 87

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 87 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is measured against the approved design baseline. The remote access path is measured against the register of exceptions. The physical controls is traced to the previous year's assessment. The segmentation boundary is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The third-party register is reconciled with the register of exceptions. The remote access path is documented alongside the dependency map. The vendor register is reviewed against the agreed service level. The monitoring pipeline is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

The physical controls is validated by the current written standard. The threat model is measured against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is traced to the most recent exercise record. The classification scheme is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The retention schedule is measured against the evidence pack held by the owner. The monitoring pipeline is measured against the dependency map. Metrics are reported as trends rather than single data points.

Plate 88

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 88 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is validated by the evidence pack held by the owner. The continuity plan is evidenced by the commissioning document. The vulnerability queue is checked against the dependency map. Each administrative account is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

The classification scheme is validated by the ticket history for the period. The identity lifecycle is evidenced by the signed exception log. The control is tested at least once every twelve months.

Every internet-facing service is reviewed against the most recent exercise record. The threat model is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The recovery test is reviewed against the current written standard. The threat model is compared with the quarterly review notes. Records are retained only as long as the schedule requires.

Each administrative account is traced to the approved design baseline. The change process is compared with the most recent exercise record. The mobile standard is reconciled with the commissioning document. The backup rotation is reconciled with the current written standard. Records are retained only as long as the schedule requires.

Plate 89

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 89 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is validated by the current written standard. The endpoint baseline is validated by the current written standard. The remote access path is evidenced by the signed exception log. The intent is to make the safe path the default rather than an exception.

The privileged access list is measured against the agreed service level. The risk register is compared with the evidence pack held by the owner. The awareness cycle is evidenced by the register of exceptions. The control is tested at least once every twelve months.

The awareness cycle is reconciled with the dependency map. The change process is reconciled with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is documented alongside the quarterly review notes. The access review process is reconciled with the ticket history for the period. The third-party register is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is checked against the most recent exercise record. The asset register is documented alongside the dependency map. The vulnerability queue is measured against the evidence pack held by the owner. The monitoring pipeline is checked against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

Plate 90

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 90 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reconciled with the previous year's assessment. The asset register is checked against the current written standard. The endpoint baseline is documented alongside the register of exceptions. The metric set is compared with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is traced to the approved design baseline. The risk register is validated by the dependency map. The retention schedule is documented alongside the most recent exercise record. The vendor register is traced to the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is measured against the ticket history for the period. The identity lifecycle is measured against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The asset register is measured against the dependency map. The privileged access list is compared with the agreed service level. The mobile standard is reconciled with the current written standard. The privileged access list is documented alongside the register of exceptions. The control is tested at least once every twelve months.

Plate 91

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 91 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is documented alongside the commissioning document. The segmentation boundary is reconciled with the signed exception log. The privileged access list is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

25. The continuity plan

The remote access path is reviewed against the ticket history for the period. The metric set is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The retention schedule is validated by the register of exceptions. The privileged access list is evidenced by the evidence pack held by the owner. The encryption standard is validated by the agreed service level. The encryption standard is evidenced by the current written standard. Metrics are reported as trends rather than single data points.

The change process is reconciled with the previous year's assessment. The threat model is documented alongside the quarterly review notes. Every internet-facing service is reviewed against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

Plate 92

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 92 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is documented alongside the agreed service level. The asset register is checked against the agreed service level. The monitoring pipeline is traced to the most recent exercise record. The vulnerability queue is reconciled with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is documented alongside the commissioning document. The identity lifecycle is documented alongside the signed exception log. The asset register is checked against the most recent exercise record. Every internet-facing service is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The access review process is documented alongside the dependency map. The monitoring pipeline is reviewed against the signed exception log. The retention schedule is documented alongside the commissioning document. The change process is reconciled with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The third-party register is reconciled with the commissioning document. The change process is documented alongside the ticket history for the period. The hardened build is reviewed against the ticket history for the period. The cloud baseline is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Plate 93

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 93 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is measured against the previous year's assessment. The recovery test is compared with the approved design baseline. The segmentation boundary is evidenced by the approved design baseline. The intent is to make the safe path the default rather than an exception.

The email authentication record is compared with the ticket history for the period. Every internet-facing service is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is traced to the agreed service level. The mobile standard is compared with the previous year's assessment. The vendor register is reviewed against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is validated by the signed exception log. The continuity plan is measured against the previous year's assessment. The continuity plan is compared with the ticket history for the period. The physical controls is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is traced to the most recent exercise record. The access review process is reconciled with the agreed service level. The procedure is written so a new starter can follow it without supervision.

Plate 94

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 94 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is traced to the commissioning document. The retention schedule is reconciled with the evidence pack held by the owner. The remote access path is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The continuity plan is reviewed against the ticket history for the period. Every internet-facing service is reviewed against the previous year's assessment. The identity lifecycle is documented alongside the previous year's assessment. Any deviation requires written approval and an expiry date.

The cloud baseline is validated by the dependency map. The hardened build is checked against the ticket history for the period. The access review process is documented alongside the ticket history for the period. The third-party register is documented alongside the quarterly review notes. Records are retained only as long as the schedule requires.

The remote access path is measured against the current written standard. The hardened build is reviewed against the approved design baseline. The cloud baseline is reviewed against the most recent exercise record. The encryption standard is traced to the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 95

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 95 - 232 x 232 px, DeviceRGB, FlateDecode

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Owner named and recorded in the register.

The risk register is reconciled with the most recent exercise record. The identity lifecycle is measured against the evidence pack held by the owner. The continuity plan is traced to the evidence pack held by the owner. The threat model is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

The remote access path is traced to the quarterly review notes. The classification scheme is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

The cloud baseline is measured against the register of exceptions. The classification scheme is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The endpoint baseline is traced to the evidence pack held by the owner. The privileged access list is validated by the register of exceptions. The mobile standard is reviewed against the signed exception log. The encryption standard is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

Plate 96

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 96 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is traced to the signed exception log. The threat model is traced to the commissioning document. The awareness cycle is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.

The endpoint baseline is measured against the evidence pack held by the owner. The cloud baseline is traced to the commissioning document. The recovery test is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

The patch calendar is reviewed against the most recent exercise record. The remote access path is traced to the dependency map. The third-party register is reconciled with the agreed service level. Any deviation requires written approval and an expiry date.

The patch calendar is evidenced by the dependency map. The mobile standard is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

Plate 97

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 97 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is traced to the approved design baseline. The endpoint baseline is compared with the signed exception log. The cloud baseline is traced to the ticket history for the period. The endpoint baseline is evidenced by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The physical controls is validated by the approved design baseline. The asset register is documented alongside the most recent exercise record. The cloud baseline is traced to the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is reconciled with the current written standard. The access review process is validated by the approved design baseline. The vendor register is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The privileged access list is traced to the current written standard. The identity lifecycle is traced to the register of exceptions. The mobile standard is measured against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 98

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 98 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is traced to the ticket history for the period. The change process is reconciled with the ticket history for the period. The encryption standard is checked against the evidence pack held by the owner. The threat model is evidenced by the register of exceptions. Third parties must demonstrate the control before access is granted.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Notification list confirmed before execution.

The vulnerability queue is reconciled with the dependency map. The risk register is traced to the approved design baseline. The mobile standard is compared with the previous year's assessment. The physical controls is evidenced by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Plate 99

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 99 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is evidenced by the most recent exercise record. The threat model is compared with the signed exception log. The awareness cycle is reviewed against the current written standard. The email authentication record is traced to the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

The cloud baseline is reviewed against the ticket history for the period. The change process is reconciled with the approved design baseline. The awareness cycle is evidenced by the quarterly review notes. The backup rotation is evidenced by the signed exception log. Records are retained only as long as the schedule requires.

The hardened build is traced to the commissioning document. The continuity plan is reviewed against the agreed service level. The mobile standard is reconciled with the register of exceptions. The privileged access list is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 100

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 100 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is compared with the agreed service level. Every internet-facing service is reviewed against the previous year's assessment. The classification scheme is measured against the evidence pack held by the owner. The recovery test is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The asset register is evidenced by the register of exceptions. The recovery test is checked against the current written standard. The threat model is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is measured against the evidence pack held by the owner. The identity lifecycle is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is evidenced by the quarterly review notes. The backup rotation is validated by the signed exception log. The metric set is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The hardened build is compared with the current written standard. The retention schedule is evidenced by the register of exceptions. The vendor register is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

Plate 101

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 101 - 232 x 232 px, DeviceRGB, FlateDecode

- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.

The asset register is documented alongside the ticket history for the period. The recovery test is compared with the ticket history for the period. The email authentication record is reconciled with the agreed service level. Every internet-facing service is evidenced by the dependency map. Any deviation requires written approval and an expiry date.

The segmentation boundary is validated by the evidence pack held by the owner. The recovery test is measured against the current written standard. Every internet-facing service is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the signed exception log. The hardened build is compared with the commissioning document. The continuity plan is evidenced by the ticket history for the period. Every internet-facing service is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

Plate 102

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 102 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is compared with the current written standard. The encryption standard is documented alongside the evidence pack held by the owner. The awareness cycle is reviewed against the register of exceptions. The patch calendar is evidenced by the agreed service level. Any deviation requires written approval and an expiry date.

The remote access path is evidenced by the approved design baseline. The patch calendar is evidenced by the current written standard. Every internet-facing service is validated by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is reviewed against the current written standard. The vulnerability queue is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The risk register is reviewed against the agreed service level. The monitoring pipeline is traced to the commissioning document. The physical controls is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The endpoint baseline is reviewed against the agreed service level. The classification scheme is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 103

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 103 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reviewed against the current written standard. The awareness cycle is documented alongside the previous year's assessment. The access review process is evidenced by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is evidenced by the evidence pack held by the owner. The email authentication record is evidenced by the dependency map. The email authentication record is reviewed against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is documented alongside the ticket history for the period. The patch calendar is compared with the evidence pack held by the owner. The control is tested at least once every twelve months.

Each administrative account is compared with the most recent exercise record. The endpoint baseline is reconciled with the register of exceptions. Every internet-facing service is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The email authentication record is validated by the register of exceptions. The endpoint baseline is reviewed against the previous year's assessment. Third parties must demonstrate the control before access is granted.

Plate 104

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 104 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is checked against the evidence pack held by the owner. The mobile standard is traced to the ticket history for the period. The remote access path is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The third-party register is validated by the commissioning document. The access review process is reconciled with the commissioning document. The vulnerability queue is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is traced to the commissioning document. The physical controls is traced to the ticket history for the period. The metric set is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The hardened build is documented alongside the commissioning document. The metric set is reconciled with the previous year's assessment. The endpoint baseline is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The email authentication record is checked against the agreed service level. The threat model is documented alongside the approved design baseline. The classification scheme is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 105

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 105 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is validated by the quarterly review notes. The privileged access list is reviewed against the dependency map. The classification scheme is evidenced by the evidence pack held by the owner. The access review process is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

The continuity plan is measured against the ticket history for the period. Each administrative account is checked against the commissioning document. The change process is documented alongside the approved design baseline. The endpoint baseline is traced to the dependency map. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is checked against the register of exceptions. The access review process is traced to the dependency map. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is reconciled with the approved design baseline. The continuity plan is reconciled with the signed exception log. The continuity plan is reviewed against the ticket history for the period. The recovery test is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Plate 106

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 106 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reviewed against the dependency map. The endpoint baseline is checked against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is validated by the approved design baseline. The encryption standard is documented alongside the commissioning document. Testing covers the failure case, not only the happy path.

The vendor register is validated by the quarterly review notes. The risk register is traced to the ticket history for the period. The segmentation boundary is validated by the approved design baseline. The remote access path is compared with the current written standard. Testing covers the failure case, not only the happy path.

Every internet-facing service is compared with the commissioning document. The email authentication record is documented alongside the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

Plate 107

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 107 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is validated by the register of exceptions. The risk register is checked against the dependency map. The change process is reviewed against the current written standard. The threat model is reconciled with the previous year's assessment. The control is tested at least once every twelve months.

- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The patch calendar is compared with the commissioning document. The identity lifecycle is compared with the dependency map. The backup rotation is evidenced by the dependency map. The recovery test is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is reviewed against the approved design baseline. The cloud baseline is traced to the agreed service level. The segmentation boundary is evidenced by the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 108

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 108 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is validated by the approved design baseline. The backup rotation is reviewed against the dependency map. The continuity plan is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is reconciled with the previous year's assessment. The endpoint baseline is reviewed against the register of exceptions. Every internet-facing service is compared with the most recent exercise record. The physical controls is measured against the previous year's assessment. The control is tested at least once every twelve months.

The vendor register is measured against the current written standard. The retention schedule is documented alongside the most recent exercise record. The email authentication record is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is compared with the dependency map. The remote access path is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is evidenced by the ticket history for the period. The endpoint baseline is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

Plate 109

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 109 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is checked against the previous year's assessment. The classification scheme is reviewed against the approved design baseline. The email authentication record is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The privileged access list is reviewed against the signed exception log. The cloud baseline is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The backup rotation is reconciled with the approved design baseline. The vulnerability queue is validated by the signed exception log. The physical controls is measured against the evidence pack held by the owner. The segmentation boundary is measured against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The change process is validated by the register of exceptions. The privileged access list is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is evidenced by the most recent exercise record. The threat model is documented alongside the register of exceptions. The physical controls is evidenced by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

Plate 110

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 110 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is compared with the approved design baseline. The monitoring pipeline is checked against the most recent exercise record. The email authentication record is checked against the most recent exercise record. The identity lifecycle is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

- Review date scheduled and visible.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The hardened build is measured against the quarterly review notes. The third-party register is reviewed against the ticket history for the period. The classification scheme is evidenced by the previous year's assessment. Records are retained only as long as the schedule requires.

The patch calendar is reconciled with the quarterly review notes. The backup rotation is reconciled with the evidence pack held by the owner. The vulnerability queue is traced to the dependency map. The classification scheme is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

Plate 111

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 111 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is validated by the current written standard. The continuity plan is checked against the current written standard. The classification scheme is documented alongside the signed exception log. The retention schedule is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The physical controls is compared with the ticket history for the period. Every internet-facing service is compared with the evidence pack held by the owner. The threat model is documented alongside the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is traced to the register of exceptions. The change process is reviewed against the previous year's assessment. The monitoring pipeline is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

The asset register is documented alongside the dependency map. The hardened build is validated by the dependency map. The vulnerability queue is documented alongside the approved design baseline. The control is tested at least once every twelve months.

Plate 112

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 112 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is measured against the approved design baseline. The vulnerability queue is reconciled with the ticket history for the period. The classification scheme is measured against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The hardened build is measured against the agreed service level. The vendor register is reconciled with the signed exception log. The access review process is compared with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.

The patch calendar is documented alongside the ticket history for the period. The vulnerability queue is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is compared with the previous year's assessment. Each administrative account is documented alongside the register of exceptions. The risk register is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

Plate 113

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 113 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is documented alongside the commissioning document. The backup rotation is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

The privileged access list is traced to the approved design baseline. The metric set is validated by the evidence pack held by the owner. The cloud baseline is documented alongside the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is compared with the most recent exercise record. The risk register is traced to the dependency map. Findings are reported to leadership in plain language, with owners and dates.

- Backup of the change retained for rollback.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Review date scheduled and visible.

Plate 114

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 114 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is validated by the previous year's assessment. The physical controls is evidenced by the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is reconciled with the dependency map. Every internet-facing service is checked against the signed exception log. The hardened build is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Test result attached to the record.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.

The continuity plan is reconciled with the approved design baseline. The retention schedule is evidenced by the agreed service level. The recovery test is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

Plate 115

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 115 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is traced to the quarterly review notes. The vulnerability queue is validated by the most recent exercise record. The backup rotation is measured against the signed exception log. The third-party register is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The threat model is reviewed against the approved design baseline. The endpoint baseline is traced to the register of exceptions. The email authentication record is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The encryption standard is reviewed against the agreed service level. The patch calendar is checked against the evidence pack held by the owner. The privileged access list is measured against the approved design baseline. The segmentation boundary is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Plate 116

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 116 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is evidenced by the signed exception log. The cloud baseline is reconciled with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is compared with the quarterly review notes. The privileged access list is documented alongside the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is compared with the agreed service level. The continuity plan is traced to the signed exception log. The monitoring pipeline is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is validated by the commissioning document. The physical controls is traced to the quarterly review notes. The recovery test is measured against the dependency map. The segmentation boundary is compared with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is traced to the ticket history for the period. The mobile standard is checked against the commissioning document. The monitoring pipeline is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

Plate 117

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 117 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reviewed against the quarterly review notes. The change process is reconciled with the signed exception log. The remote access path is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is traced to the agreed service level. The continuity plan is validated by the current written standard. The patch calendar is reconciled with the quarterly review notes. The hardened build is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

Each administrative account is validated by the commissioning document. The threat model is reconciled with the evidence pack held by the owner. The email authentication record is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Plate 118

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 118 - 232 x 232 px, DeviceRGB, FlateDecode

28. The classification scheme

The risk register is documented alongside the signed exception log. The change process is reviewed against the dependency map. The vulnerability queue is checked against the ticket history for the period. The vendor register is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The asset register is validated by the signed exception log. The vulnerability queue is validated by the approved design baseline. The privileged access list is documented alongside the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The change process is traced to the signed exception log. The threat model is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is reviewed against the quarterly review notes. The privileged access list is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

The hardened build is reviewed against the ticket history for the period. The third-party register is traced to the dependency map. The access review process is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

Plate 119

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 119 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is documented alongside the approved design baseline. The vulnerability queue is reviewed against the current written standard. The risk register is checked against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The third-party register is traced to the signed exception log. The recovery test is compared with the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is checked against the register of exceptions. The backup rotation is measured against the evidence pack held by the owner. The awareness cycle is measured against the register of exceptions. The control is tested at least once every twelve months.

Every internet-facing service is compared with the commissioning document. The remote access path is checked against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

Plate 120

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 120 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is documented alongside the dependency map. The third-party register is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is measured against the evidence pack held by the owner. The threat model is measured against the dependency map. The classification scheme is traced to the ticket history for the period. Metrics are reported as trends rather than single data points.

The awareness cycle is documented alongside the ticket history for the period. The change process is traced to the dependency map. The identity lifecycle is reviewed against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

29. The asset register

The access review process is reconciled with the agreed service level. The hardened build is measured against the register of exceptions. The third-party register is traced to the commissioning document. Every internet-facing service is checked against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 121

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 121 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is measured against the previous year's assessment. Each administrative account is documented alongside the dependency map. The email authentication record is measured against the approved design baseline. Metrics are reported as trends rather than single data points.

The backup rotation is traced to the register of exceptions. The third-party register is documented alongside the most recent exercise record. The physical controls is checked against the quarterly review notes. Each administrative account is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the evidence pack held by the owner. The email authentication record is documented alongside the most recent exercise record. The endpoint baseline is evidenced by the current written standard. The mobile standard is evidenced by the current written standard. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is reconciled with the agreed service level. The vulnerability queue is evidenced by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is compared with the signed exception log. The backup rotation is evidenced by the approved design baseline. Records are retained only as long as the schedule requires.

Plate 122

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 122 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is reconciled with the register of exceptions. The segmentation boundary is reconciled with the current written standard. The awareness cycle is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is traced to the approved design baseline. The continuity plan is compared with the register of exceptions. The segmentation boundary is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

The vendor register is compared with the ticket history for the period. The segmentation boundary is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is traced to the current written standard. The encryption standard is documented alongside the signed exception log. The change process is validated by the agreed service level. The physical controls is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Plate 123

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 123 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is measured against the signed exception log. The retention schedule is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is compared with the agreed service level. The patch calendar is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The backup rotation is reconciled with the quarterly review notes. The encryption standard is measured against the register of exceptions. The classification scheme is reconciled with the ticket history for the period. The email authentication record is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The encryption standard is validated by the signed exception log. The classification scheme is reviewed against the most recent exercise record. The backup rotation is reconciled with the previous year's assessment. The retention schedule is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The risk register is traced to the agreed service level. The backup rotation is documented alongside the register of exceptions. The segmentation boundary is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Plate 124

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 124 - 232 x 232 px, DeviceRGB, FlateDecode

- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The recovery test is documented alongside the dependency map. Every internet-facing service is documented alongside the register of exceptions. The backup rotation is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is reviewed against the ticket history for the period. The physical controls is checked against the evidence pack held by the owner. The classification scheme is reconciled with the most recent exercise record. The encryption standard is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is compared with the commissioning document. The email authentication record is measured against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

Plate 125

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 125 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is evidenced by the agreed service level. The retention schedule is validated by the commissioning document. The access review process is checked against the evidence pack held by the owner. The threat model is checked against the previous year's assessment. Records are retained only as long as the schedule requires.

The recovery test is documented alongside the dependency map. The remote access path is compared with the quarterly review notes. Each administrative account is reviewed against the signed exception log. The asset register is reconciled with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is traced to the signed exception log. The segmentation boundary is checked against the quarterly review notes. The segmentation boundary is traced to the quarterly review notes. The identity lifecycle is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is compared with the dependency map. The privileged access list is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

Plate 126

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 126 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is compared with the approved design baseline. Every internet-facing service is reconciled with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is traced to the most recent exercise record. The segmentation boundary is checked against the register of exceptions. Third parties must demonstrate the control before access is granted.

The continuity plan is reconciled with the current written standard. The retention schedule is compared with the current written standard. The physical controls is checked against the quarterly review notes. The identity lifecycle is validated by the approved design baseline. Records are retained only as long as the schedule requires.

Each administrative account is documented alongside the ticket history for the period. The identity lifecycle is validated by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Plate 127

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 127 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is validated by the dependency map. The continuity plan is checked against the current written standard. The vendor register is measured against the current written standard. The control is tested at least once every twelve months.

The cloud baseline is reconciled with the agreed service level. The asset register is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

- Test result attached to the record.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The identity lifecycle is validated by the most recent exercise record. The change process is validated by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 128

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 128 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is traced to the previous year's assessment. The email authentication record is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The hardened build is traced to the commissioning document. The endpoint baseline is checked against the ticket history for the period. The threat model is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The encryption standard is measured against the register of exceptions. The vendor register is reconciled with the previous year's assessment. The segmentation boundary is validated by the agreed service level. The continuity plan is compared with the signed exception log. Testing covers the failure case, not only the happy path.

The segmentation boundary is traced to the agreed service level. The encryption standard is reconciled with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

Plate 129

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 129 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is validated by the evidence pack held by the owner. Each administrative account is reviewed against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

30. Each administrative account

The hardened build is reviewed against the most recent exercise record. The retention schedule is validated by the most recent exercise record. The asset register is checked against the approved design baseline. Any deviation requires written approval and an expiry date.

The endpoint baseline is documented alongside the most recent exercise record. The vendor register is traced to the ticket history for the period. The classification scheme is traced to the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

31. The metric set

The retention schedule is validated by the most recent exercise record. The vulnerability queue is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

Plate 130

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 130 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is documented alongside the signed exception log. The identity lifecycle is validated by the ticket history for the period. The mobile standard is documented alongside the register of exceptions. The continuity plan is validated by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is measured against the current written standard. The patch calendar is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The change process is validated by the ticket history for the period. The change process is documented alongside the register of exceptions. The risk register is reviewed against the ticket history for the period. The retention schedule is compared with the agreed service level. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.

Plate 131

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 131 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is documented alongside the most recent exercise record. The hardened build is reviewed against the evidence pack held by the owner. The continuity plan is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is compared with the most recent exercise record. The segmentation boundary is traced to the evidence pack held by the owner. The physical controls is checked against the most recent exercise record. The awareness cycle is compared with the current written standard. The control is tested at least once every twelve months.

The cloud baseline is reconciled with the commissioning document. The cloud baseline is documented alongside the register of exceptions. The segmentation boundary is evidenced by the register of exceptions. The intent is to make the safe path the default rather than an exception.

32. The cloud baseline

The asset register is validated by the evidence pack held by the owner. The encryption standard is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

Plate 132

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 132 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is traced to the dependency map. The classification scheme is reconciled with the agreed service level. The third-party register is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is measured against the current written standard. The retention schedule is evidenced by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is reconciled with the ticket history for the period. Every internet-facing service is traced to the ticket history for the period. The monitoring pipeline is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is reviewed against the dependency map. The awareness cycle is traced to the evidence pack held by the owner. The classification scheme is compared with the most recent exercise record. The segmentation boundary is validated by the previous year's assessment. Third parties must demonstrate the control before access is granted.

Plate 133

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 133 - 232 x 232 px, DeviceRGB, FlateDecode

33. The third-party register

The privileged access list is validated by the previous year's assessment. The classification scheme is checked against the quarterly review notes. The recovery test is validated by the quarterly review notes. The recovery test is checked against the agreed service level. Records are retained only as long as the schedule requires.

The metric set is reconciled with the ticket history for the period. The cloud baseline is checked against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The access review process is documented alongside the previous year's assessment. The physical controls is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

Every internet-facing service is checked against the quarterly review notes. Each administrative account is evidenced by the dependency map. The email authentication record is evidenced by the previous year's assessment. The third-party register is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Plate 134

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 134 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is reviewed against the previous year's assessment. Each administrative account is measured against the approved design baseline. The monitoring pipeline is reconciled with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is validated by the dependency map. The continuity plan is validated by the evidence pack held by the owner. The awareness cycle is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

Each administrative account is checked against the most recent exercise record. The backup rotation is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is reviewed against the approved design baseline. The email authentication record is measured against the ticket history for the period. The backup rotation is compared with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is documented alongside the quarterly review notes. The patch calendar is reconciled with the register of exceptions. The continuity plan is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

Plate 135

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 135 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is checked against the approved design baseline. The third-party register is traced to the signed exception log. The monitoring pipeline is validated by the previous year's assessment. The remote access path is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The access review process is validated by the quarterly review notes. The endpoint baseline is measured against the signed exception log. The physical controls is validated by the signed exception log. Records are retained only as long as the schedule requires.

The privileged access list is measured against the signed exception log. The email authentication record is evidenced by the agreed service level. Every internet-facing service is checked against the commissioning document. The control is tested at least once every twelve months.

- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

The privileged access list is reviewed against the previous year's assessment. The vulnerability queue is checked against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Plate 136

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 136 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is traced to the signed exception log. The hardened build is checked against the register of exceptions. The third-party register is compared with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The change process is validated by the evidence pack held by the owner. The threat model is reconciled with the approved design baseline. The awareness cycle is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is reconciled with the quarterly review notes. The endpoint baseline is validated by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The risk register is traced to the ticket history for the period. The access review process is checked against the most recent exercise record. The third-party register is compared with the evidence pack held by the owner. The vendor register is traced to the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is checked against the previous year's assessment. The backup rotation is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 137

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 137 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is measured against the ticket history for the period. The encryption standard is reconciled with the evidence pack held by the owner. The vendor register is traced to the quarterly review notes. The third-party register is checked against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The mobile standard is reconciled with the current written standard. The metric set is reconciled with the register of exceptions. Every internet-facing service is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

Every internet-facing service is evidenced by the ticket history for the period. The identity lifecycle is reviewed against the current written standard. Each administrative account is evidenced by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is evidenced by the most recent exercise record. The change process is reconciled with the signed exception log. The threat model is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

Plate 138

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 138 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is measured against the signed exception log. The access review process is documented alongside the agreed service level. The patch calendar is measured against the quarterly review notes. The physical controls is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The identity lifecycle is compared with the signed exception log. The physical controls is reviewed against the ticket history for the period. The asset register is checked against the agreed service level. Records are retained only as long as the schedule requires.

The vendor register is checked against the current written standard. The asset register is validated by the current written standard. Third parties must demonstrate the control before access is granted.

Every internet-facing service is measured against the evidence pack held by the owner. The encryption standard is measured against the commissioning document. The third-party register is validated by the dependency map. The encryption standard is validated by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is evidenced by the register of exceptions. The continuity plan is validated by the ticket history for the period. The vulnerability queue is traced to the previous year's assessment. Any deviation requires written approval and an expiry date.

Plate 139

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 139 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is checked against the ticket history for the period. The asset register is evidenced by the previous year's assessment. The metric set is traced to the commissioning document. The mobile standard is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The identity lifecycle is measured against the agreed service level. The change process is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is reconciled with the agreed service level. The third-party register is evidenced by the previous year's assessment. The awareness cycle is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The segmentation boundary is reviewed against the evidence pack held by the owner. The endpoint baseline is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The threat model is checked against the ticket history for the period. The privileged access list is compared with the approved design baseline. The retention schedule is checked against the current written standard. The retention schedule is traced to the signed exception log. Records are retained only as long as the schedule requires.

Plate 140

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 140 - 232 x 232 px, DeviceRGB, FlateDecode

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The endpoint baseline is traced to the ticket history for the period. The retention schedule is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

The retention schedule is compared with the current written standard. The continuity plan is validated by the previous year's assessment. Every internet-facing service is reviewed against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The metric set is validated by the most recent exercise record. The recovery test is checked against the signed exception log. Records are retained only as long as the schedule requires.

The access review process is compared with the dependency map. The continuity plan is reviewed against the approved design baseline. The recovery test is evidenced by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Plate 141

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 141 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is compared with the previous year's assessment. The physical controls is reviewed against the commissioning document. The vulnerability queue is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The threat model is evidenced by the signed exception log. The vendor register is checked against the ticket history for the period. Records are retained only as long as the schedule requires.

The endpoint baseline is documented alongside the previous year's assessment. The risk register is validated by the most recent exercise record. The asset register is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Test result attached to the record.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

Plate 142

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 142 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is measured against the evidence pack held by the owner. Every internet-facing service is evidenced by the approved design baseline. The email authentication record is compared with the previous year's assessment. Testing covers the failure case, not only the happy path.

The third-party register is reconciled with the most recent exercise record. The asset register is measured against the dependency map. The patch calendar is measured against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The third-party register is checked against the quarterly review notes. The vulnerability queue is reviewed against the previous year's assessment. The cloud baseline is checked against the current written standard. Third parties must demonstrate the control before access is granted.

The segmentation boundary is measured against the most recent exercise record. The change process is reconciled with the most recent exercise record. The mobile standard is validated by the most recent exercise record. The monitoring pipeline is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

Plate 143

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 143 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is validated by the current written standard. The monitoring pipeline is reviewed against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The third-party register is measured against the evidence pack held by the owner. The patch calendar is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is evidenced by the previous year's assessment. The patch calendar is compared with the register of exceptions. The risk register is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is measured against the signed exception log. The access review process is evidenced by the ticket history for the period. The third-party register is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The privileged access list is traced to the quarterly review notes. Every internet-facing service is reconciled with the current written standard. The access review process is validated by the agreed service level. The patch calendar is checked against the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 144

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 144 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is traced to the commissioning document. The hardened build is evidenced by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The change process is reconciled with the approved design baseline. The remote access path is measured against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The risk register is measured against the evidence pack held by the owner. The metric set is measured against the signed exception log. The metric set is traced to the dependency map. Testing covers the failure case, not only the happy path.

The endpoint baseline is reviewed against the evidence pack held by the owner. The change process is measured against the signed exception log. Each administrative account is compared with the most recent exercise record. The risk register is documented alongside the dependency map. Records are retained only as long as the schedule requires.

The metric set is evidenced by the agreed service level. The retention schedule is checked against the evidence pack held by the owner. The asset register is compared with the agreed service level. Any deviation requires written approval and an expiry date.

Plate 145

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 145 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is traced to the signed exception log. Each administrative account is evidenced by the agreed service level. The encryption standard is traced to the quarterly review notes. Each administrative account is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is reconciled with the dependency map. The monitoring pipeline is compared with the current written standard. Metrics are reported as trends rather than single data points.

34. The mobile standard

The threat model is evidenced by the agreed service level. The monitoring pipeline is measured against the approved design baseline. The segmentation boundary is reconciled with the agreed service level. The retention schedule is reconciled with the register of exceptions. Metrics are reported as trends rather than single data points.

- Test result attached to the record.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

Plate 146

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 146 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is documented alongside the most recent exercise record. The privileged access list is measured against the ticket history for the period. The backup rotation is validated by the dependency map. Any deviation requires written approval and an expiry date.

The access review process is checked against the approved design baseline. The access review process is validated by the register of exceptions. The endpoint baseline is compared with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is reviewed against the commissioning document. The awareness cycle is traced to the signed exception log. The encryption standard is validated by the signed exception log. The risk register is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The change process is evidenced by the previous year's assessment. The metric set is checked against the signed exception log. The awareness cycle is reconciled with the agreed service level. The third-party register is evidenced by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

Plate 147

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 147 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is traced to the register of exceptions. The vulnerability queue is traced to the register of exceptions. The email authentication record is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

35. The privileged access list

The risk register is reviewed against the agreed service level. The risk register is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is checked against the current written standard. The mobile standard is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is validated by the register of exceptions. Every internet-facing service is traced to the ticket history for the period. The third-party register is compared with the commissioning document. The change process is validated by the commissioning document. The procedure is written so a new starter can follow it without supervision.

Plate 148

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 148 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is checked against the dependency map. Each administrative account is checked against the most recent exercise record. The retention schedule is evidenced by the quarterly review notes. The asset register is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The threat model is validated by the register of exceptions. The monitoring pipeline is reconciled with the evidence pack held by the owner. The monitoring pipeline is measured against the dependency map. The identity lifecycle is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The metric set is checked against the quarterly review notes. The physical controls is traced to the commissioning document. The control is tested at least once every twelve months.

The segmentation boundary is validated by the ticket history for the period. The patch calendar is documented alongside the ticket history for the period. The endpoint baseline is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 149

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 149 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is measured against the evidence pack held by the owner. The physical controls is evidenced by the most recent exercise record. The hardened build is evidenced by the most recent exercise record. The access review process is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The backup rotation is reconciled with the most recent exercise record. The threat model is evidenced by the ticket history for the period. The cloud baseline is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The retention schedule is checked against the commissioning document. The cloud baseline is evidenced by the previous year's assessment. The retention schedule is compared with the current written standard. Any deviation requires written approval and an expiry date.

The patch calendar is measured against the quarterly review notes. The privileged access list is validated by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

Plate 150

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 150 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is checked against the register of exceptions. Each administrative account is evidenced by the previous year's assessment. The vulnerability queue is checked against the agreed service level. Each administrative account is traced to the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is validated by the commissioning document. The third-party register is measured against the dependency map. Every internet-facing service is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is measured against the dependency map. The cloud baseline is reviewed against the signed exception log. Each administrative account is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is reconciled with the approved design baseline. The threat model is checked against the commissioning document. The vendor register is measured against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

Plate 151

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 151 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is reconciled with the register of exceptions. The hardened build is reconciled with the register of exceptions. The third-party register is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Review date scheduled and visible.

The awareness cycle is traced to the evidence pack held by the owner. The cloud baseline is evidenced by the register of exceptions. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the quarterly review notes. Each administrative account is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reconciled with the most recent exercise record. Each administrative account is evidenced by the ticket history for the period. The vulnerability queue is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

Plate 152

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 152 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is documented alongside the commissioning document. The physical controls is measured against the approved design baseline. The cloud baseline is evidenced by the dependency map. The classification scheme is measured against the current written standard. Metrics are reported as trends rather than single data points.

The classification scheme is measured against the approved design baseline. The risk register is reconciled with the previous year's assessment. The mobile standard is compared with the most recent exercise record. Third parties must demonstrate the control before access is granted.

Each administrative account is reconciled with the current written standard. Each administrative account is reconciled with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The change process is evidenced by the approved design baseline. The vulnerability queue is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is evidenced by the approved design baseline. The segmentation boundary is traced to the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Plate 153

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 153 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is traced to the most recent exercise record. The cloud baseline is compared with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is checked against the register of exceptions. The hardened build is evidenced by the agreed service level. The identity lifecycle is reconciled with the ticket history for the period. Any deviation requires written approval and an expiry date.

The change process is traced to the ticket history for the period. The encryption standard is checked against the signed exception log. The physical controls is documented alongside the previous year's assessment. The vendor register is traced to the quarterly review notes. Metrics are reported as trends rather than single data points.

The mobile standard is traced to the register of exceptions. Each administrative account is measured against the dependency map. The backup rotation is checked against the evidence pack held by the owner. The physical controls is checked against the commissioning document. Any deviation requires written approval and an expiry date.

Each administrative account is reconciled with the current written standard. The email authentication record is reconciled with the current written standard. The classification scheme is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

Plate 154

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 154 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is validated by the signed exception log. The physical controls is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is reviewed against the approved design baseline. The patch calendar is checked against the register of exceptions. The third-party register is evidenced by the current written standard. The control is tested at least once every twelve months.

The change process is compared with the current written standard. The access review process is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is reconciled with the current written standard. The vendor register is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The asset register is compared with the evidence pack held by the owner. The access review process is documented alongside the most recent exercise record. The encryption standard is measured against the previous year's assessment. The third-party register is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

Plate 155

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 155 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is validated by the most recent exercise record. The third-party register is compared with the current written standard. The backup rotation is reconciled with the commissioning document. Every internet-facing service is reviewed against the approved design baseline. Any deviation requires written approval and an expiry date.

The access review process is validated by the register of exceptions. The mobile standard is evidenced by the current written standard. The remote access path is validated by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is checked against the agreed service level. The cloud baseline is reconciled with the commissioning document. The change process is reconciled with the agreed service level. The asset register is evidenced by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The threat model is checked against the register of exceptions. The vendor register is validated by the evidence pack held by the owner. The recovery test is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

Plate 156

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 156 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is documented alongside the approved design baseline. The monitoring pipeline is reviewed against the agreed service level. The retention schedule is checked against the quarterly review notes. The recovery test is validated by the current written standard. Any deviation requires written approval and an expiry date.

The classification scheme is traced to the current written standard. The mobile standard is traced to the current written standard. The threat model is compared with the approved design baseline. The recovery test is evidenced by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

- Review date scheduled and visible.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.

The vendor register is checked against the current written standard. The segmentation boundary is compared with the approved design baseline. The continuity plan is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 157

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 157 - 232 x 232 px, DeviceRGB, FlateDecode

37. The monitoring pipeline

The monitoring pipeline is checked against the current written standard. The change process is evidenced by the previous year's assessment. The access review process is evidenced by the approved design baseline. The awareness cycle is measured against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is traced to the dependency map. The retention schedule is measured against the register of exceptions. The cloud baseline is evidenced by the dependency map. The remote access path is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is measured against the most recent exercise record. The threat model is compared with the agreed service level. The threat model is traced to the register of exceptions. The procedure is written so a new starter can follow it without supervision.

Plate 158

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 158 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is checked against the signed exception log. The classification scheme is measured against the commissioning document. The recovery test is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The third-party register is reviewed against the current written standard. The change process is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Test result attached to the record.
- Exception route documented and time-bound.

The asset register is validated by the dependency map. The endpoint baseline is reconciled with the register of exceptions. The mobile standard is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

Plate 159

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 159 - 232 x 232 px, DeviceRGB, FlateDecode

38. The email authentication record

The continuity plan is traced to the register of exceptions. The recovery test is measured against the dependency map. The continuity plan is measured against the register of exceptions. The control is tested at least once every twelve months.

The retention schedule is evidenced by the most recent exercise record. The classification scheme is reconciled with the evidence pack held by the owner. The endpoint baseline is compared with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The physical controls is reviewed against the evidence pack held by the owner. The vulnerability queue is compared with the register of exceptions. The mobile standard is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is traced to the previous year's assessment. The access review process is reviewed against the dependency map. The cloud baseline is documented alongside the approved design baseline. The change process is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

Plate 160

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 160 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is compared with the signed exception log. The email authentication record is measured against the previous year's assessment. Testing covers the failure case, not only the happy path.

- Exception route documented and time-bound.
- Test result attached to the record.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The segmentation boundary is traced to the ticket history for the period. The cloud baseline is reconciled with the current written standard. The metric set is measured against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is validated by the current written standard. The asset register is measured against the register of exceptions. The mobile standard is checked against the commissioning document. Metrics are reported as trends rather than single data points.

Plate 161

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 161 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is reconciled with the current written standard. The hardened build is documented alongside the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Acceptance criteria written before work starts.

The change process is checked against the commissioning document. The email authentication record is documented alongside the quarterly review notes. The metric set is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the register of exceptions. The awareness cycle is validated by the register of exceptions. The risk register is measured against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 162

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 162 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is checked against the agreed service level. The remote access path is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The access review process is measured against the quarterly review notes. The backup rotation is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The mobile standard is documented alongside the evidence pack held by the owner. The physical controls is compared with the register of exceptions. The email authentication record is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 163

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 163 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is evidenced by the evidence pack held by the owner. The privileged access list is reconciled with the ticket history for the period. The metric set is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is measured against the most recent exercise record. The awareness cycle is documented alongside the commissioning document. Each administrative account is checked against the previous year's assessment. The metric set is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The change process is evidenced by the previous year's assessment. The email authentication record is documented alongside the signed exception log. The physical controls is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

40. The threat model

The endpoint baseline is evidenced by the evidence pack held by the owner. The vendor register is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 164

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 164 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the dependency map. The physical controls is compared with the quarterly review notes. The change process is compared with the commissioning document. The procedure is written so a new starter can follow it without supervision.

The email authentication record is reviewed against the previous year's assessment. The email authentication record is evidenced by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is compared with the commissioning document. The encryption standard is reviewed against the approved design baseline. The monitoring pipeline is checked against the agreed service level. The patch calendar is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is traced to the register of exceptions. The recovery test is reviewed against the most recent exercise record. The remote access path is documented alongside the evidence pack held by the owner. The segmentation boundary is checked against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

Plate 165

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 165 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is compared with the register of exceptions. The email authentication record is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

The vulnerability queue is validated by the approved design baseline. The continuity plan is evidenced by the agreed service level. The physical controls is reviewed against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is evidenced by the agreed service level. The threat model is evidenced by the previous year's assessment. The identity lifecycle is documented alongside the dependency map. The risk register is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is reviewed against the most recent exercise record. Every internet-facing service is documented alongside the agreed service level. The backup rotation is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The metric set is reviewed against the current written standard. The retention schedule is traced to the commissioning document. The change process is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

Plate 166

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 166 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is documented alongside the dependency map. The vulnerability queue is validated by the agreed service level. The identity lifecycle is reconciled with the previous year's assessment. The encryption standard is measured against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The risk register is reconciled with the quarterly review notes. The encryption standard is validated by the ticket history for the period. The classification scheme is compared with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

- Test result attached to the record.
- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Review date scheduled and visible.

Plate 167

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 167 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is measured against the dependency map. The mobile standard is evidenced by the evidence pack held by the owner. The segmentation boundary is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The metric set is documented alongside the current written standard. The privileged access list is reviewed against the previous year's assessment. The monitoring pipeline is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is evidenced by the previous year's assessment. The awareness cycle is evidenced by the current written standard. The change process is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is validated by the previous year's assessment. The backup rotation is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The access review process is reconciled with the quarterly review notes. The recovery test is reconciled with the dependency map. The vendor register is evidenced by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

Plate 168

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 168 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is documented alongside the previous year's assessment. The backup rotation is validated by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

42. The physical controls

The monitoring pipeline is documented alongside the register of exceptions. The email authentication record is measured against the current written standard. The encryption standard is traced to the previous year's assessment. The endpoint baseline is measured against the commissioning document. The intent is to make the safe path the default rather than an exception.

The hardened build is evidenced by the dependency map. The backup rotation is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is validated by the ticket history for the period. The third-party register is compared with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Plate 169

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 169 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is reviewed against the most recent exercise record. The monitoring pipeline is reconciled with the commissioning document. The awareness cycle is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The vendor register is evidenced by the approved design baseline. The continuity plan is traced to the ticket history for the period. The privileged access list is checked against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The threat model is compared with the evidence pack held by the owner. The access review process is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The access review process is measured against the quarterly review notes. The classification scheme is validated by the register of exceptions. The endpoint baseline is documented alongside the current written standard. The metric set is measured against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The risk register is traced to the agreed service level. The backup rotation is traced to the current written standard. Every internet-facing service is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

Plate 170

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 170 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is evidenced by the current written standard. The access review process is checked against the approved design baseline. The continuity plan is traced to the agreed service level. Records are retained only as long as the schedule requires.

Each administrative account is traced to the agreed service level. The mobile standard is reconciled with the signed exception log. The privileged access list is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The encryption standard is reviewed against the most recent exercise record. The access review process is validated by the agreed service level. The email authentication record is compared with the evidence pack held by the owner. The vulnerability queue is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

43. The backup rotation

The threat model is reviewed against the signed exception log. The vulnerability queue is reconciled with the previous year's assessment. The email authentication record is measured against the commissioning document. The patch calendar is measured against the current written standard. Records are retained only as long as the schedule requires.

Plate 171

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 171 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is validated by the previous year's assessment. The asset register is evidenced by the quarterly review notes. The cloud baseline is reviewed against the ticket history for the period. The recovery test is validated by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is evidenced by the agreed service level. Every internet-facing service is documented alongside the most recent exercise record. The endpoint baseline is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is checked against the quarterly review notes. The threat model is validated by the ticket history for the period. The vendor register is documented alongside the evidence pack held by the owner. The identity lifecycle is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The threat model is reviewed against the agreed service level. The vendor register is checked against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

Plate 172

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 172 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is documented alongside the most recent exercise record. The email authentication record is traced to the dependency map. The classification scheme is traced to the commissioning document. The change process is reviewed against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is documented alongside the most recent exercise record. The access review process is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is measured against the commissioning document. The privileged access list is documented alongside the agreed service level. The privileged access list is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is measured against the previous year's assessment. The encryption standard is reconciled with the current written standard. The patch calendar is documented alongside the agreed service level. The email authentication record is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

Plate 173

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 173 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is measured against the ticket history for the period. The access review process is evidenced by the approved design baseline. The metric set is compared with the approved design baseline. The retention schedule is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is validated by the register of exceptions. The access review process is checked against the signed exception log. The vulnerability queue is evidenced by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is checked against the previous year's assessment. The awareness cycle is documented alongside the ticket history for the period. The monitoring pipeline is traced to the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The change process is validated by the previous year's assessment. The email authentication record is validated by the signed exception log. Records are retained only as long as the schedule requires.

- Review date scheduled and visible.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.

Plate 174

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 174 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is traced to the quarterly review notes. The segmentation boundary is reconciled with the agreed service level. The metric set is checked against the signed exception log. Metrics are reported as trends rather than single data points.

The identity lifecycle is reviewed against the commissioning document. The endpoint baseline is validated by the previous year's assessment. The control is tested at least once every twelve months.

The access review process is documented alongside the register of exceptions. The endpoint baseline is validated by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is checked against the evidence pack held by the owner. Each administrative account is documented alongside the register of exceptions. The physical controls is validated by the signed exception log. Testing covers the failure case, not only the happy path.

The segmentation boundary is measured against the agreed service level. The metric set is reconciled with the commissioning document. The threat model is compared with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

Plate 175

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 175 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is validated by the commissioning document. The vulnerability queue is reviewed against the evidence pack held by the owner. The change process is validated by the ticket history for the period. The email authentication record is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The asset register is validated by the current written standard. The encryption standard is checked against the signed exception log. The awareness cycle is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is measured against the quarterly review notes. The retention schedule is checked against the register of exceptions. The cloud baseline is validated by the commissioning document. Metrics are reported as trends rather than single data points.

The risk register is compared with the previous year's assessment. The privileged access list is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

Each administrative account is checked against the quarterly review notes. The identity lifecycle is measured against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

Plate 176

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 176 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is checked against the commissioning document. Every internet-facing service is compared with the most recent exercise record. Every internet-facing service is evidenced by the ticket history for the period. Testing covers the failure case, not only the happy path.

The third-party register is traced to the signed exception log. The vendor register is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The change process is measured against the commissioning document. The privileged access list is reconciled with the most recent exercise record. The identity lifecycle is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The hardened build is evidenced by the quarterly review notes. The mobile standard is checked against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is documented alongside the agreed service level. The vulnerability queue is reconciled with the register of exceptions. The continuity plan is evidenced by the approved design baseline. The control is tested at least once every twelve months.

Plate 177

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 177 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is measured against the ticket history for the period. The endpoint baseline is documented alongside the current written standard. The metric set is documented alongside the current written standard. The hardened build is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reviewed against the signed exception log. The change process is reviewed against the commissioning document. Any deviation requires written approval and an expiry date.

The mobile standard is traced to the current written standard. The mobile standard is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The threat model is reviewed against the agreed service level. The retention schedule is reviewed against the evidence pack held by the owner. The control is tested at least once every twelve months.

- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.

The metric set is reviewed against the signed exception log. The identity lifecycle is traced to the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

Plate 178

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 178 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is reconciled with the current written standard. The vendor register is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The asset register is measured against the current written standard. The asset register is measured against the commissioning document. The change process is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The classification scheme is evidenced by the ticket history for the period. The risk register is compared with the signed exception log. The remote access path is reviewed against the signed exception log. The email authentication record is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

The awareness cycle is reconciled with the register of exceptions. The monitoring pipeline is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is validated by the ticket history for the period. The hardened build is reviewed against the agreed service level. Third parties must demonstrate the control before access is granted.

Plate 179

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 179 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is validated by the dependency map. The access review process is reconciled with the previous year's assessment. The continuity plan is validated by the commissioning document. The control is tested at least once every twelve months.

The hardened build is traced to the signed exception log. The threat model is checked against the ticket history for the period. Each administrative account is compared with the most recent exercise record. The third-party register is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The awareness cycle is measured against the agreed service level. The patch calendar is traced to the commissioning document. The vulnerability queue is reviewed against the current written standard. The change process is compared with the dependency map. Any deviation requires written approval and an expiry date.

The encryption standard is measured against the register of exceptions. The change process is compared with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

Plate 180

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 180 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is documented alongside the register of exceptions. The awareness cycle is measured against the commissioning document. The email authentication record is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is checked against the evidence pack held by the owner. The classification scheme is traced to the most recent exercise record. The cloud baseline is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The threat model is reviewed against the ticket history for the period. Each administrative account is measured against the approved design baseline. The privileged access list is documented alongside the evidence pack held by the owner. The classification scheme is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The threat model is documented alongside the previous year's assessment. The vulnerability queue is reconciled with the previous year's assessment. The threat model is documented alongside the ticket history for the period. The access review process is traced to the commissioning document. The procedure is written so a new starter can follow it without supervision.

Plate 181

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 181 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is reconciled with the most recent exercise record. The remote access path is checked against the dependency map. The segmentation boundary is compared with the current written standard. The remote access path is evidenced by the current written standard. The control is tested at least once every twelve months.

The change process is validated by the evidence pack held by the owner. The backup rotation is measured against the approved design baseline. The continuity plan is measured against the evidence pack held by the owner. The remote access path is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The mobile standard is measured against the approved design baseline. The monitoring pipeline is compared with the dependency map. The access review process is compared with the previous year's assessment. The continuity plan is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The recovery test is validated by the signed exception log. The risk register is traced to the commissioning document. The third-party register is measured against the signed exception log. The continuity plan is measured against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

Plate 182

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 182 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is validated by the approved design baseline. The privileged access list is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The asset register is reviewed against the commissioning document. The vendor register is compared with the signed exception log. The identity lifecycle is measured against the approved design baseline. Each administrative account is validated by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The recovery test is reconciled with the most recent exercise record. The segmentation boundary is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The recovery test is checked against the quarterly review notes. The physical controls is measured against the agreed service level. The intent is to make the safe path the default rather than an exception.

The retention schedule is traced to the signed exception log. The email authentication record is compared with the agreed service level. The change process is evidenced by the agreed service level. The monitoring pipeline is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

Plate 183

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 183 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is reconciled with the approved design baseline. The physical controls is traced to the evidence pack held by the owner. The monitoring pipeline is traced to the evidence pack held by the owner. The change process is reconciled with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is traced to the approved design baseline. The remote access path is compared with the dependency map. The vendor register is reviewed against the quarterly review notes. The backup rotation is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.

The hardened build is measured against the current written standard. The cloud baseline is validated by the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 184

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 184 - 232 x 232 px, DeviceRGB, FlateDecode

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.

The identity lifecycle is validated by the quarterly review notes. The mobile standard is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is traced to the current written standard. The retention schedule is reviewed against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The vendor register is checked against the dependency map. The recovery test is evidenced by the evidence pack held by the owner. The asset register is compared with the current written standard. The physical controls is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

Plate 185

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 185 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is evidenced by the most recent exercise record. The third-party register is traced to the quarterly review notes. The threat model is documented alongside the register of exceptions. The remote access path is measured against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The email authentication record is traced to the signed exception log. The access review process is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The physical controls is reconciled with the commissioning document. The email authentication record is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The hardened build is reviewed against the ticket history for the period. The cloud baseline is reconciled with the quarterly review notes. Each administrative account is reconciled with the current written standard. The metric set is compared with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is traced to the previous year's assessment. The privileged access list is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 186

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 186 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is evidenced by the evidence pack held by the owner. The mobile standard is measured against the most recent exercise record. The classification scheme is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The classification scheme is reconciled with the evidence pack held by the owner. The hardened build is traced to the most recent exercise record. The hardened build is checked against the ticket history for the period. The cloud baseline is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the evidence pack held by the owner. The identity lifecycle is reconciled with the previous year's assessment. The threat model is traced to the ticket history for the period. The control is tested at least once every twelve months.

The access review process is measured against the ticket history for the period. The cloud baseline is documented alongside the register of exceptions. The segmentation boundary is evidenced by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 187

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 187 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is compared with the most recent exercise record. The classification scheme is traced to the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is traced to the register of exceptions. The asset register is evidenced by the commissioning document. The encryption standard is validated by the register of exceptions. The vendor register is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is checked against the quarterly review notes. The encryption standard is traced to the dependency map. The asset register is measured against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reconciled with the evidence pack held by the owner. The third-party register is evidenced by the current written standard. The patch calendar is measured against the approved design baseline. The cloud baseline is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Plate 188

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 188 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is documented alongside the evidence pack held by the owner. The patch calendar is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is reconciled with the commissioning document. The segmentation boundary is validated by the commissioning document. The physical controls is checked against the current written standard. Any deviation requires written approval and an expiry date.

The privileged access list is traced to the approved design baseline. The vulnerability queue is reconciled with the evidence pack held by the owner. The control is tested at least once every twelve months.

46. The vendor register

The remote access path is evidenced by the previous year's assessment. The monitoring pipeline is measured against the agreed service level. The retention schedule is compared with the ticket history for the period. The threat model is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

Plate 189

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 189 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is compared with the ticket history for the period. Every internet-facing service is checked against the register of exceptions. The third-party register is documented alongside the register of exceptions. The vendor register is evidenced by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is documented alongside the ticket history for the period. The identity lifecycle is measured against the approved design baseline. The segmentation boundary is validated by the register of exceptions. The continuity plan is validated by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is compared with the agreed service level. The mobile standard is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

The recovery test is validated by the current written standard. The continuity plan is measured against the current written standard. The third-party register is reconciled with the evidence pack held by the owner. The classification scheme is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The asset register is validated by the agreed service level. Every internet-facing service is reconciled with the signed exception log. Third parties must demonstrate the control before access is granted.

Plate 190

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 190 - 232 x 232 px, DeviceRGB, FlateDecode

- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The privileged access list is validated by the commissioning document. The patch calendar is evidenced by the approved design baseline. The hardened build is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The remote access path is compared with the approved design baseline. The mobile standard is validated by the dependency map. The awareness cycle is checked against the commissioning document. The remote access path is evidenced by the register of exceptions. Records are retained only as long as the schedule requires.

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

Plate 191

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 191 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is documented alongside the previous year's assessment. The mobile standard is validated by the approved design baseline. The endpoint baseline is evidenced by the previous year's assessment. The awareness cycle is evidenced by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The asset register is measured against the quarterly review notes. The asset register is evidenced by the register of exceptions. Any deviation requires written approval and an expiry date.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.

The monitoring pipeline is documented alongside the commissioning document. The vulnerability queue is evidenced by the previous year's assessment. The privileged access list is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

Plate 192

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 192 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is validated by the previous year's assessment. The cloud baseline is checked against the quarterly review notes. The metric set is evidenced by the previous year's assessment. The endpoint baseline is reviewed against the previous year's assessment. Any deviation requires written approval and an expiry date.

The threat model is reconciled with the evidence pack held by the owner. The backup rotation is reconciled with the most recent exercise record. The physical controls is traced to the dependency map. The email authentication record is evidenced by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The threat model is checked against the agreed service level. The hardened build is documented alongside the agreed service level. The risk register is documented alongside the current written standard. Testing covers the failure case, not only the happy path.

Each administrative account is reconciled with the approved design baseline. The asset register is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

Plate 193

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 193 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is traced to the approved design baseline. The backup rotation is compared with the evidence pack held by the owner. The awareness cycle is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

48. The change process

The asset register is measured against the previous year's assessment. The access review process is documented alongside the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is checked against the quarterly review notes. The asset register is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

The encryption standard is documented alongside the register of exceptions. The patch calendar is evidenced by the dependency map. The segmentation boundary is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The recovery test is evidenced by the current written standard. The monitoring pipeline is checked against the previous year's assessment. Testing covers the failure case, not only the happy path.

Plate 194

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 194 - 232 x 232 px, DeviceRGB, FlateDecode

49. The mobile standard

The mobile standard is measured against the current written standard. The privileged access list is measured against the most recent exercise record. The patch calendar is measured against the current written standard. The procedure is written so a new starter can follow it without supervision.

The risk register is evidenced by the dependency map. The physical controls is reviewed against the dependency map. The identity lifecycle is compared with the agreed service level. The email authentication record is measured against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The threat model is evidenced by the dependency map. The recovery test is measured against the register of exceptions. The patch calendar is validated by the most recent exercise record. The segmentation boundary is reconciled with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Plate 195

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 195 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is validated by the evidence pack held by the owner. The recovery test is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the ticket history for the period. Every internet-facing service is reconciled with the quarterly review notes. The continuity plan is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reviewed against the approved design baseline. The email authentication record is documented alongside the agreed service level. The physical controls is documented alongside the signed exception log. The retention schedule is evidenced by the quarterly review notes. Records are retained only as long as the schedule requires.

The vulnerability queue is evidenced by the evidence pack held by the owner. The physical controls is documented alongside the ticket history for the period. The metric set is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is validated by the current written standard. The continuity plan is compared with the most recent exercise record. The cloud baseline is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Plate 196

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 196 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is reviewed against the signed exception log. The monitoring pipeline is traced to the quarterly review notes. The privileged access list is compared with the signed exception log. The physical controls is reviewed against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is reconciled with the ticket history for the period. The backup rotation is reconciled with the evidence pack held by the owner. The monitoring pipeline is traced to the current written standard. Records are retained only as long as the schedule requires.

- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.

The recovery test is reconciled with the agreed service level. The vendor register is documented alongside the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

Plate 197

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 197 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is compared with the quarterly review notes. The endpoint baseline is checked against the dependency map. The control is tested at least once every twelve months.

50. The physical controls

The asset register is validated by the quarterly review notes. The awareness cycle is evidenced by the evidence pack held by the owner. The identity lifecycle is reviewed against the evidence pack held by the owner. The backup rotation is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

51. The retention schedule

The continuity plan is traced to the register of exceptions. The continuity plan is compared with the current written standard. The control is tested at least once every twelve months.

Every internet-facing service is checked against the approved design baseline. Every internet-facing service is traced to the dependency map. The identity lifecycle is measured against the agreed service level. Any deviation requires written approval and an expiry date.

Plate 198

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 198 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the commissioning document. The privileged access list is traced to the most recent exercise record. The mobile standard is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is traced to the signed exception log. The backup rotation is reviewed against the previous year's assessment. The physical controls is evidenced by the evidence pack held by the owner. The endpoint baseline is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The classification scheme is reviewed against the agreed service level. The email authentication record is validated by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is compared with the agreed service level. The vulnerability queue is reconciled with the commissioning document. The third-party register is checked against the dependency map. The mobile standard is checked against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 199

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 199 - 232 x 232 px, DeviceRGB, FlateDecode

52. The continuity plan

The access review process is checked against the evidence pack held by the owner. The threat model is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The access review process is validated by the previous year's assessment. The backup rotation is compared with the approved design baseline. The awareness cycle is reconciled with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The third-party register is validated by the register of exceptions. The change process is traced to the dependency map. The hardened build is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

The third-party register is traced to the most recent exercise record. The privileged access list is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 200

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 200 - 232 x 232 px, DeviceRGB, FlateDecode

- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.

The threat model is traced to the ticket history for the period. The cloud baseline is traced to the commissioning document. The patch calendar is compared with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is traced to the ticket history for the period. The patch calendar is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is documented alongside the dependency map. The encryption standard is reconciled with the ticket history for the period. The continuity plan is traced to the quarterly review notes. The third-party register is validated by the current written standard. The measure applies equally to staff, contractors and managed service providers.

Plate 201

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 201 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is measured against the evidence pack held by the owner. The physical controls is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

The backup rotation is evidenced by the register of exceptions. The segmentation boundary is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is reviewed against the most recent exercise record. The email authentication record is reviewed against the quarterly review notes. The third-party register is checked against the signed exception log. The remote access path is documented alongside the agreed service level. The control is tested at least once every twelve months.

The change process is measured against the approved design baseline. The endpoint baseline is compared with the evidence pack held by the owner. The continuity plan is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

Plate 202

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 202 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is checked against the quarterly review notes. The threat model is compared with the previous year's assessment. The metric set is traced to the commissioning document. Any deviation requires written approval and an expiry date.

The cloud baseline is checked against the approved design baseline. Every internet-facing service is measured against the current written standard. The privileged access list is documented alongside the current written standard. The recovery test is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Review date scheduled and visible.

The patch calendar is reconciled with the previous year's assessment. The endpoint baseline is checked against the approved design baseline. The threat model is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Plate 203

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 203 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the evidence pack held by the owner. The remote access path is validated by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is compared with the agreed service level. The physical controls is measured against the signed exception log. The retention schedule is traced to the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The remote access path is reviewed against the agreed service level. The remote access path is compared with the dependency map. The awareness cycle is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is documented alongside the register of exceptions. The retention schedule is reviewed against the register of exceptions. The email authentication record is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is compared with the agreed service level. The recovery test is reconciled with the ticket history for the period. The cloud baseline is traced to the dependency map. Third parties must demonstrate the control before access is granted.

Plate 204

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 204 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is checked against the approved design baseline. The asset register is checked against the current written standard. The change process is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

The access review process is traced to the current written standard. The monitoring pipeline is measured against the evidence pack held by the owner. The email authentication record is checked against the commissioning document. The threat model is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is checked against the register of exceptions. The change process is evidenced by the register of exceptions. The asset register is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The physical controls is reviewed against the most recent exercise record. The identity lifecycle is evidenced by the evidence pack held by the owner. The continuity plan is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The backup rotation is reviewed against the quarterly review notes. The change process is traced to the current written standard. Exceptions are costly by design: they expire and must be re-justified.

Plate 205

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 205 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is reviewed against the ticket history for the period. The encryption standard is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The threat model is reviewed against the most recent exercise record. The change process is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is traced to the dependency map. The mobile standard is evidenced by the dependency map. The threat model is documented alongside the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The change process is measured against the approved design baseline. The third-party register is reconciled with the current written standard. The awareness cycle is reviewed against the approved design baseline. The endpoint baseline is traced to the most recent exercise record. Testing covers the failure case, not only the happy path.

The risk register is measured against the previous year's assessment. The endpoint baseline is documented alongside the signed exception log. Every internet-facing service is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

Plate 206

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 206 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is traced to the previous year's assessment. The identity lifecycle is reviewed against the previous year's assessment. The backup rotation is checked against the current written standard. The endpoint baseline is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is evidenced by the agreed service level. Every internet-facing service is evidenced by the quarterly review notes. The continuity plan is compared with the register of exceptions. The mobile standard is measured against the most recent exercise record. Records are retained only as long as the schedule requires.

The mobile standard is evidenced by the ticket history for the period. The classification scheme is reconciled with the register of exceptions. The third-party register is compared with the agreed service level. Each administrative account is reviewed against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is validated by the evidence pack held by the owner. The cloud baseline is reviewed against the approved design baseline. The endpoint baseline is traced to the agreed service level. The vendor register is checked against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 207

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 207 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is reconciled with the most recent exercise record. The endpoint baseline is documented alongside the agreed service level. The email authentication record is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is traced to the evidence pack held by the owner. The privileged access list is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

The third-party register is compared with the approved design baseline. The privileged access list is documented alongside the most recent exercise record. Every internet-facing service is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The privileged access list is documented alongside the quarterly review notes. The threat model is reconciled with the register of exceptions. The monitoring pipeline is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Plate 208

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 208 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is traced to the current written standard. The email authentication record is validated by the agreed service level. The endpoint baseline is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is documented alongside the dependency map. The asset register is traced to the previous year's assessment. The access review process is compared with the evidence pack held by the owner. The continuity plan is documented alongside the approved design baseline. Any deviation requires written approval and an expiry date.

The email authentication record is reconciled with the commissioning document. The awareness cycle is documented alongside the quarterly review notes. Each administrative account is compared with the signed exception log. The access review process is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

Every internet-facing service is traced to the dependency map. The classification scheme is reconciled with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 209

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 209 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is evidenced by the agreed service level. The hardened build is reconciled with the dependency map. The intent is to make the safe path the default rather than an exception.

53. The segmentation boundary

The monitoring pipeline is reviewed against the current written standard. The continuity plan is validated by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The asset register is reviewed against the signed exception log. The awareness cycle is traced to the previous year's assessment. The mobile standard is reconciled with the previous year's assessment. The privileged access list is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is validated by the most recent exercise record. The patch calendar is checked against the signed exception log. The hardened build is reconciled with the evidence pack held by the owner. The cloud baseline is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

Plate 210

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 210 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is documented alongside the previous year's assessment. The endpoint baseline is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The metric set is measured against the signed exception log. The segmentation boundary is reviewed against the previous year's assessment. The privileged access list is traced to the signed exception log. The vendor register is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Owner named and recorded in the register.

The vendor register is documented alongside the evidence pack held by the owner. The monitoring pipeline is reconciled with the dependency map. The privileged access list is validated by the commissioning document. The procedure is written so a new starter can follow it without supervision.

Plate 211

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 211 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is validated by the commissioning document. The hardened build is evidenced by the commissioning document. The access review process is reviewed against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The metric set is traced to the agreed service level. The threat model is compared with the quarterly review notes. The awareness cycle is compared with the quarterly review notes. Metrics are reported as trends rather than single data points.

The threat model is evidenced by the dependency map. The risk register is validated by the quarterly review notes. Each administrative account is measured against the previous year's assessment. The segmentation boundary is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

Plate 212

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 212 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is measured against the register of exceptions. The mobile standard is checked against the current written standard. The vulnerability queue is checked against the register of exceptions. The awareness cycle is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The email authentication record is reconciled with the approved design baseline. Each administrative account is reconciled with the previous year's assessment. Metrics are reported as trends rather than single data points.

The vendor register is reviewed against the most recent exercise record. The backup rotation is documented alongside the commissioning document. The recovery test is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

Plate 213

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 213 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is documented alongside the register of exceptions. The asset register is traced to the register of exceptions. The continuity plan is traced to the commissioning document. The classification scheme is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The change process is traced to the dependency map. Each administrative account is reconciled with the ticket history for the period. The identity lifecycle is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The threat model is measured against the register of exceptions. The change process is evidenced by the register of exceptions. The vulnerability queue is compared with the register of exceptions. The control is tested at least once every twelve months.

The asset register is checked against the evidence pack held by the owner. The vendor register is validated by the ticket history for the period. The patch calendar is documented alongside the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 214

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 214 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is compared with the previous year's assessment. The vendor register is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is measured against the previous year's assessment. The segmentation boundary is evidenced by the previous year's assessment. The awareness cycle is compared with the ticket history for the period. Metrics are reported as trends rather than single data points.

The retention schedule is evidenced by the most recent exercise record. The asset register is checked against the signed exception log. The retention schedule is checked against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the agreed service level. The privileged access list is documented alongside the ticket history for the period. The metric set is checked against the dependency map. The control is tested at least once every twelve months.

Plate 215

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 215 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is validated by the ticket history for the period. The patch calendar is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reviewed against the commissioning document. The vendor register is reconciled with the register of exceptions. The awareness cycle is validated by the commissioning document. The endpoint baseline is validated by the signed exception log. Any deviation requires written approval and an expiry date.

The metric set is checked against the dependency map. The patch calendar is compared with the evidence pack held by the owner. The awareness cycle is reviewed against the evidence pack held by the owner. The threat model is evidenced by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The email authentication record is documented alongside the register of exceptions. The email authentication record is validated by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Plate 216

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 216 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is validated by the ticket history for the period. The vendor register is traced to the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The endpoint baseline is checked against the commissioning document. Each administrative account is validated by the evidence pack held by the owner. The privileged access list is measured against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is reviewed against the agreed service level. The patch calendar is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The metric set is validated by the agreed service level. The risk register is evidenced by the most recent exercise record. The privileged access list is compared with the agreed service level. The risk register is reviewed against the commissioning document. Testing covers the failure case, not only the happy path.

The identity lifecycle is evidenced by the agreed service level. The segmentation boundary is reconciled with the commissioning document. The threat model is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

Plate 217

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 217 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is evidenced by the current written standard. The patch calendar is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

54. The identity lifecycle

The remote access path is reconciled with the register of exceptions. The mobile standard is reconciled with the commissioning document. The segmentation boundary is measured against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The change process is measured against the register of exceptions. The metric set is validated by the commissioning document. The awareness cycle is measured against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The threat model is traced to the commissioning document. The identity lifecycle is measured against the commissioning document. The control is tested at least once every twelve months.

Plate 218

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 218 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is measured against the most recent exercise record. The monitoring pipeline is compared with the evidence pack held by the owner. Each administrative account is documented alongside the dependency map. The identity lifecycle is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

The cloud baseline is documented alongside the approved design baseline. The vendor register is checked against the previous year's assessment. The retention schedule is traced to the approved design baseline. The change process is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is documented alongside the signed exception log. The threat model is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

The asset register is reconciled with the most recent exercise record. The metric set is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The recovery test is documented alongside the signed exception log. The hardened build is measured against the evidence pack held by the owner. The encryption standard is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

Plate 219

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 219 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is evidenced by the current written standard. The metric set is checked against the most recent exercise record. The metric set is measured against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The metric set is traced to the current written standard. The awareness cycle is validated by the commissioning document. The monitoring pipeline is traced to the register of exceptions. The recovery test is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The hardened build is measured against the approved design baseline. The vulnerability queue is measured against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The remote access path is traced to the agreed service level. The identity lifecycle is compared with the dependency map. Testing covers the failure case, not only the happy path.

The mobile standard is validated by the current written standard. Every internet-facing service is validated by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Plate 220

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 220 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is validated by the approved design baseline. The vendor register is measured against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is compared with the dependency map. The vendor register is validated by the commissioning document. The retention schedule is measured against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The hardened build is traced to the commissioning document. The asset register is reconciled with the dependency map. The vulnerability queue is validated by the dependency map. The recovery test is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is compared with the quarterly review notes. The remote access path is reconciled with the current written standard. The endpoint baseline is checked against the previous year's assessment. Each administrative account is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The classification scheme is checked against the signed exception log. The mobile standard is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

Plate 221

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 221 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is traced to the previous year's assessment. The access review process is evidenced by the ticket history for the period. The change process is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is reconciled with the dependency map. Every internet-facing service is documented alongside the approved design baseline. The privileged access list is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The segmentation boundary is measured against the most recent exercise record. The mobile standard is compared with the agreed service level. The privileged access list is reconciled with the previous year's assessment. The endpoint baseline is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is measured against the current written standard. The hardened build is checked against the signed exception log. Records are retained only as long as the schedule requires.

The change process is measured against the most recent exercise record. The hardened build is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 222

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 222 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is compared with the dependency map. The awareness cycle is traced to the signed exception log. The change process is traced to the agreed service level. The metric set is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The email authentication record is reviewed against the quarterly review notes. The recovery test is reviewed against the signed exception log. The retention schedule is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The privileged access list is traced to the approved design baseline. The email authentication record is traced to the approved design baseline. The endpoint baseline is validated by the current written standard. The vendor register is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is traced to the current written standard. The mobile standard is documented alongside the signed exception log. The remote access path is traced to the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Plate 223

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 223 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is validated by the register of exceptions. The physical controls is traced to the evidence pack held by the owner. The privileged access list is traced to the dependency map. The remote access path is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.

The email authentication record is traced to the previous year's assessment. The endpoint baseline is compared with the signed exception log. The email authentication record is documented alongside the commissioning document. Testing covers the failure case, not only the happy path.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

Plate 224

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 224 - 232 x 232 px, DeviceRGB, FlateDecode

55. The continuity plan

The third-party register is documented alongside the signed exception log. The segmentation boundary is reviewed against the previous year's assessment. Records are retained only as long as the schedule requires.

The cloud baseline is traced to the most recent exercise record. The asset register is documented alongside the dependency map. The risk register is documented alongside the current written standard. The change process is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The segmentation boundary is traced to the dependency map. The backup rotation is compared with the evidence pack held by the owner. The hardened build is evidenced by the current written standard. The backup rotation is measured against the commissioning document. Records are retained only as long as the schedule requires.

Plate 225

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 225 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is reconciled with the ticket history for the period. The identity lifecycle is compared with the ticket history for the period. The monitoring pipeline is measured against the agreed service level. The threat model is evidenced by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is compared with the ticket history for the period. The email authentication record is compared with the register of exceptions. The risk register is evidenced by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is measured against the ticket history for the period. The third-party register is checked against the register of exceptions. The mobile standard is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is evidenced by the most recent exercise record. The privileged access list is reconciled with the approved design baseline. The remote access path is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is evidenced by the current written standard. The privileged access list is checked against the approved design baseline. The endpoint baseline is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 226

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 226 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is evidenced by the quarterly review notes. The metric set is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is compared with the approved design baseline. The continuity plan is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The monitoring pipeline is measured against the agreed service level. The backup rotation is validated by the approved design baseline. The access review process is reconciled with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The asset register is documented alongside the evidence pack held by the owner. The vulnerability queue is checked against the current written standard. The remote access path is compared with the agreed service level. The vulnerability queue is checked against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is reviewed against the ticket history for the period. The threat model is traced to the evidence pack held by the owner. Every internet-facing service is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Plate 227

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 227 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is checked against the commissioning document. The continuity plan is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reconciled with the previous year's assessment. The classification scheme is compared with the approved design baseline. The physical controls is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is measured against the approved design baseline. The backup rotation is checked against the commissioning document. The vulnerability queue is compared with the ticket history for the period. The privileged access list is traced to the agreed service level. Testing covers the failure case, not only the happy path.

56. The endpoint baseline

The segmentation boundary is traced to the register of exceptions. The change process is checked against the agreed service level. Any deviation requires written approval and an expiry date.

Plate 228

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 228 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is evidenced by the dependency map. The threat model is traced to the most recent exercise record. The patch calendar is documented alongside the current written standard. The asset register is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The physical controls is validated by the ticket history for the period. The cloud baseline is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

The threat model is measured against the quarterly review notes. Every internet-facing service is reconciled with the current written standard. The endpoint baseline is compared with the signed exception log. Each administrative account is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

Every internet-facing service is reconciled with the current written standard. The physical controls is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

Plate 229

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 229 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is measured against the evidence pack held by the owner. The change process is reviewed against the ticket history for the period. The asset register is measured against the current written standard. The cloud baseline is documented alongside the register of exceptions. Third parties must demonstrate the control before access is granted.

The change process is checked against the dependency map. The recovery test is compared with the dependency map. Testing covers the failure case, not only the happy path.

Each administrative account is reconciled with the evidence pack held by the owner. The privileged access list is reviewed against the approved design baseline. Every internet-facing service is reconciled with the agreed service level. The threat model is measured against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The vendor register is checked against the evidence pack held by the owner. The email authentication record is documented alongside the agreed service level. The continuity plan is documented alongside the commissioning document. The classification scheme is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 230

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 230 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is traced to the approved design baseline. The threat model is validated by the current written standard. The physical controls is evidenced by the register of exceptions. The retention schedule is validated by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The mobile standard is evidenced by the commissioning document. The change process is measured against the signed exception log. The vulnerability queue is checked against the approved design baseline. The metric set is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The access review process is evidenced by the dependency map. The endpoint baseline is measured against the dependency map. The endpoint baseline is compared with the most recent exercise record. The physical controls is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is compared with the signed exception log. The privileged access list is compared with the agreed service level. The encryption standard is evidenced by the dependency map. Third parties must demonstrate the control before access is granted.

Plate 231

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 231 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is traced to the most recent exercise record. The patch calendar is evidenced by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The physical controls is checked against the current written standard. The vendor register is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The threat model is reviewed against the commissioning document. The mobile standard is evidenced by the signed exception log. The encryption standard is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Plate 232

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 232 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is measured against the ticket history for the period. The awareness cycle is validated by the dependency map. Any deviation requires written approval and an expiry date.

Each administrative account is checked against the ticket history for the period. Every internet-facing service is validated by the ticket history for the period. Metrics are reported as trends rather than single data points.

The awareness cycle is evidenced by the agreed service level. The cloud baseline is evidenced by the commissioning document. The threat model is traced to the previous year's assessment. The identity lifecycle is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

57. The identity lifecycle

The patch calendar is measured against the signed exception log. The threat model is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

Plate 233

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 233 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is measured against the evidence pack held by the owner. The backup rotation is reconciled with the register of exceptions. The patch calendar is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

The physical controls is reconciled with the evidence pack held by the owner. The mobile standard is evidenced by the register of exceptions. Each administrative account is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

The hardened build is traced to the commissioning document. The change process is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

The vulnerability queue is measured against the most recent exercise record. The change process is measured against the register of exceptions. The hardened build is evidenced by the ticket history for the period. The mobile standard is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The physical controls is documented alongside the dependency map. The physical controls is reviewed against the quarterly review notes. The control is tested at least once every twelve months.

Plate 234

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 234 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is reconciled with the quarterly review notes. The backup rotation is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The email authentication record is validated by the quarterly review notes. The mobile standard is reconciled with the register of exceptions. The classification scheme is checked against the ticket history for the period. The recovery test is reconciled with the previous year's assessment. Testing covers the failure case, not only the happy path.

The asset register is reconciled with the agreed service level. The retention schedule is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is reconciled with the register of exceptions. The mobile standard is documented alongside the dependency map. The metric set is compared with the approved design baseline. The cloud baseline is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

Each administrative account is reconciled with the signed exception log. The physical controls is reconciled with the quarterly review notes. The third-party register is reconciled with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

Plate 235

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 235 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is evidenced by the evidence pack held by the owner. The third-party register is validated by the ticket history for the period. The control is tested at least once every twelve months.

The identity lifecycle is traced to the current written standard. The privileged access list is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The asset register is checked against the previous year's assessment. The encryption standard is measured against the quarterly review notes. The threat model is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

The access review process is checked against the most recent exercise record. The endpoint baseline is checked against the ticket history for the period. The recovery test is reviewed against the approved design baseline. The segmentation boundary is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The metric set is evidenced by the signed exception log. The identity lifecycle is traced to the most recent exercise record. The recovery test is reconciled with the agreed service level. Every internet-facing service is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 236

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 236 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is documented alongside the current written standard. The asset register is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The encryption standard is checked against the register of exceptions. The classification scheme is evidenced by the signed exception log. The metric set is checked against the dependency map. The vulnerability queue is traced to the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is validated by the approved design baseline. The email authentication record is compared with the commissioning document. Testing covers the failure case, not only the happy path.

The metric set is validated by the most recent exercise record. The monitoring pipeline is measured against the most recent exercise record. The identity lifecycle is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the current written standard. The vulnerability queue is measured against the signed exception log. The metric set is traced to the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 237

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 237 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is evidenced by the commissioning document. Every internet-facing service is traced to the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The cloud baseline is evidenced by the ticket history for the period. The access review process is validated by the approved design baseline. Every internet-facing service is checked against the signed exception log. The awareness cycle is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

58. The encryption standard

The email authentication record is reviewed against the approved design baseline. The awareness cycle is measured against the quarterly review notes. The change process is compared with the agreed service level. Every internet-facing service is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is checked against the signed exception log. The retention schedule is traced to the agreed service level. The continuity plan is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

Plate 238

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 238 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is documented alongside the commissioning document. The backup rotation is compared with the agreed service level. The encryption standard is reviewed against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is reviewed against the most recent exercise record. The metric set is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The risk register is measured against the register of exceptions. The privileged access list is compared with the signed exception log. The continuity plan is checked against the register of exceptions. The identity lifecycle is traced to the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The access review process is evidenced by the commissioning document. Each administrative account is checked against the register of exceptions. The change process is documented alongside the approved design baseline. The change process is evidenced by the approved design baseline. The control is tested at least once every twelve months.

Plate 239

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 239 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is traced to the quarterly review notes. The backup rotation is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The threat model is documented alongside the ticket history for the period. The email authentication record is checked against the most recent exercise record. The cloud baseline is compared with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

59. The third-party register

The email authentication record is reviewed against the most recent exercise record. The backup rotation is evidenced by the most recent exercise record. The awareness cycle is evidenced by the current written standard. The physical controls is reviewed against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is compared with the signed exception log. The privileged access list is measured against the previous year's assessment. The privileged access list is reviewed against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

Plate 240

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 240 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is validated by the ticket history for the period. The recovery test is traced to the ticket history for the period. The privileged access list is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The change process is traced to the dependency map. The threat model is validated by the most recent exercise record. The metric set is validated by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is reconciled with the approved design baseline. The vendor register is compared with the dependency map. Any deviation requires written approval and an expiry date.

The asset register is evidenced by the evidence pack held by the owner. The mobile standard is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is measured against the dependency map. The vulnerability queue is checked against the signed exception log. The intent is to make the safe path the default rather than an exception.

Plate 241

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 241 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is validated by the previous year's assessment. The continuity plan is compared with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is validated by the ticket history for the period. The asset register is checked against the current written standard. The asset register is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is evidenced by the previous year's assessment. The privileged access list is documented alongside the dependency map. Any deviation requires written approval and an expiry date.

The privileged access list is reviewed against the signed exception log. The threat model is evidenced by the most recent exercise record. The vendor register is reconciled with the evidence pack held by the owner. The identity lifecycle is checked against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is checked against the ticket history for the period. The segmentation boundary is checked against the evidence pack held by the owner. The control is tested at least once every twelve months.

Plate 242

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 242 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is measured against the previous year's assessment. The recovery test is reviewed against the quarterly review notes. The awareness cycle is documented alongside the evidence pack held by the owner. Every internet-facing service is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The vendor register is checked against the approved design baseline. The change process is evidenced by the register of exceptions. The mobile standard is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is validated by the current written standard. The mobile standard is compared with the agreed service level. The privileged access list is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

The hardened build is documented alongside the commissioning document. The physical controls is validated by the signed exception log. The awareness cycle is validated by the ticket history for the period. The threat model is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is traced to the agreed service level. The continuity plan is evidenced by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Plate 243

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 243 - 232 x 232 px, DeviceRGB, FlateDecode

60. The hardened build

The recovery test is compared with the previous year's assessment. The access review process is documented alongside the ticket history for the period. Each administrative account is traced to the most recent exercise record. Testing covers the failure case, not only the happy path.

The backup rotation is traced to the ticket history for the period. The backup rotation is checked against the commissioning document. The endpoint baseline is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The remote access path is checked against the commissioning document. The third-party register is validated by the previous year's assessment. The patch calendar is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is checked against the register of exceptions. The third-party register is checked against the approved design baseline. The recovery test is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

Plate 244

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 244 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is evidenced by the signed exception log. The metric set is validated by the current written standard. Every internet-facing service is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The recovery test is reconciled with the signed exception log. The vulnerability queue is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is measured against the approved design baseline. The mobile standard is validated by the quarterly review notes. Any deviation requires written approval and an expiry date.

The cloud baseline is measured against the quarterly review notes. The vendor register is measured against the register of exceptions. Records are retained only as long as the schedule requires.

The backup rotation is compared with the ticket history for the period. The email authentication record is reconciled with the ticket history for the period. The privileged access list is measured against the most recent exercise record. The control is tested at least once every twelve months.

Plate 245

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 245 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is measured against the quarterly review notes. The mobile standard is measured against the most recent exercise record. The endpoint baseline is reconciled with the dependency map. The classification scheme is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The remote access path is evidenced by the approved design baseline. The awareness cycle is measured against the most recent exercise record. Any deviation requires written approval and an expiry date.

The hardened build is reconciled with the dependency map. The segmentation boundary is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The physical controls is evidenced by the agreed service level. The vendor register is reconciled with the quarterly review notes. The encryption standard is reviewed against the quarterly review notes. The mobile standard is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Plate 246

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 246 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is measured against the current written standard. The physical controls is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The change process is evidenced by the ticket history for the period. The awareness cycle is reviewed against the current written standard. The monitoring pipeline is documented alongside the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is reviewed against the evidence pack held by the owner. The recovery test is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

The privileged access list is traced to the quarterly review notes. The privileged access list is reconciled with the previous year's assessment. The physical controls is documented alongside the commissioning document. The threat model is evidenced by the ticket history for the period. Records are retained only as long as the schedule requires.

- Test result attached to the record.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

Plate 247

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 247 - 232 x 232 px, DeviceRGB, FlateDecode

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Test result attached to the record.
- Notification list confirmed before execution.

Each administrative account is reviewed against the dependency map. The cloud baseline is measured against the agreed service level. The backup rotation is traced to the register of exceptions. The third-party register is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The hardened build is documented alongside the ticket history for the period. The hardened build is evidenced by the approved design baseline. Each administrative account is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Plate 248

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 248 - 232 x 232 px, DeviceRGB, FlateDecode

61. The cloud baseline

The physical controls is checked against the agreed service level. The monitoring pipeline is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is evidenced by the register of exceptions. The endpoint baseline is reconciled with the dependency map. The email authentication record is compared with the agreed service level. The segmentation boundary is reconciled with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The remote access path is evidenced by the signed exception log. The backup rotation is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is reviewed against the ticket history for the period. The segmentation boundary is reviewed against the signed exception log. The endpoint baseline is evidenced by the approved design baseline. The recovery test is validated by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Plate 249

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 249 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is traced to the register of exceptions. Each administrative account is reconciled with the commissioning document. The physical controls is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is reviewed against the most recent exercise record. The cloud baseline is validated by the most recent exercise record. Each administrative account is traced to the current written standard. The retention schedule is validated by the current written standard. Records are retained only as long as the schedule requires.

Every internet-facing service is compared with the current written standard. The retention schedule is measured against the previous year's assessment. The vendor register is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.

The change process is traced to the dependency map. The access review process is documented alongside the agreed service level. The intent is to make the safe path the default rather than an exception.

Plate 250

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 250 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is measured against the quarterly review notes. The awareness cycle is checked against the quarterly review notes. Each administrative account is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is documented alongside the signed exception log. The patch calendar is measured against the previous year's assessment. The awareness cycle is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The mobile standard is reviewed against the register of exceptions. The threat model is measured against the agreed service level. Metrics are reported as trends rather than single data points.

62. The risk register

The endpoint baseline is traced to the evidence pack held by the owner. The identity lifecycle is reconciled with the commissioning document. The access review process is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The backup rotation is reviewed against the signed exception log. The vulnerability queue is checked against the commissioning document. The risk register is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

Plate 251

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 251 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is compared with the signed exception log. The retention schedule is reconciled with the dependency map. The segmentation boundary is documented alongside the agreed service level. The mobile standard is measured against the current written standard. The control is tested at least once every twelve months.

The metric set is reconciled with the register of exceptions. The vendor register is evidenced by the agreed service level. The cloud baseline is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

63. The mobile standard

The patch calendar is validated by the dependency map. The classification scheme is validated by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is compared with the ticket history for the period. The mobile standard is measured against the commissioning document. The intent is to make the safe path the default rather than an exception.

Plate 252

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 252 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is validated by the commissioning document. The threat model is documented alongside the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is reviewed against the approved design baseline. The backup rotation is validated by the dependency map. Testing covers the failure case, not only the happy path.

The cloud baseline is evidenced by the dependency map. The segmentation boundary is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is documented alongside the signed exception log. The mobile standard is validated by the most recent exercise record. The privileged access list is compared with the current written standard. The remote access path is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

The identity lifecycle is measured against the signed exception log. The remote access path is reviewed against the commissioning document. The encryption standard is measured against the commissioning document. The control is tested at least once every twelve months.

Plate 253

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 253 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is reconciled with the register of exceptions. The hardened build is documented alongside the current written standard. The cloud baseline is validated by the signed exception log. The access review process is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The physical controls is evidenced by the register of exceptions. The third-party register is checked against the agreed service level. Third parties must demonstrate the control before access is granted.

The cloud baseline is evidenced by the current written standard. The change process is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is validated by the signed exception log. The email authentication record is reviewed against the most recent exercise record. The encryption standard is traced to the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The threat model is evidenced by the approved design baseline. Each administrative account is checked against the evidence pack held by the owner. The endpoint baseline is measured against the commissioning document. The access review process is traced to the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Plate 254

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 254 - 232 x 232 px, DeviceRGB, FlateDecode

- Backup of the change retained for rollback.
- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

Each administrative account is reconciled with the current written standard. The endpoint baseline is evidenced by the most recent exercise record. The third-party register is evidenced by the agreed service level. The control is tested at least once every twelve months.

The remote access path is reconciled with the register of exceptions. The cloud baseline is reviewed against the signed exception log. The patch calendar is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The privileged access list is evidenced by the register of exceptions. The endpoint baseline is measured against the previous year's assessment. The classification scheme is compared with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

Plate 255

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 255 - 232 x 232 px, DeviceRGB, FlateDecode

64. The third-party register

The asset register is measured against the previous year's assessment. The awareness cycle is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The third-party register is measured against the agreed service level. The change process is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is reconciled with the previous year's assessment. Every internet-facing service is evidenced by the commissioning document. The mobile standard is traced to the quarterly review notes. The segmentation boundary is reviewed against the current written standard. The control is tested at least once every twelve months.

The remote access path is checked against the register of exceptions. The physical controls is compared with the approved design baseline. The recovery test is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Plate 256

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 256 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is traced to the evidence pack held by the owner. The vendor register is reviewed against the register of exceptions. The cloud baseline is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the signed exception log. The mobile standard is evidenced by the register of exceptions. The recovery test is reviewed against the most recent exercise record. The third-party register is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The privileged access list is compared with the approved design baseline. The hardened build is validated by the commissioning document. The metric set is reconciled with the previous year's assessment. The control is tested at least once every twelve months.

The asset register is traced to the signed exception log. The asset register is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

Each administrative account is checked against the dependency map. Every internet-facing service is traced to the register of exceptions. The encryption standard is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

Plate 257

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 257 - 232 x 232 px, DeviceRGB, FlateDecode

65. The remote access path

The retention schedule is measured against the previous year's assessment. The asset register is measured against the register of exceptions. The cloud baseline is reviewed against the commissioning document. The classification scheme is evidenced by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is checked against the commissioning document. The risk register is reconciled with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The metric set is traced to the agreed service level. The metric set is checked against the commissioning document. Each administrative account is reviewed against the evidence pack held by the owner. The hardened build is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The identity lifecycle is checked against the ticket history for the period. The identity lifecycle is compared with the dependency map. Any deviation requires written approval and an expiry date.

Plate 258

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 258 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is traced to the previous year's assessment. The segmentation boundary is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The vendor register is reviewed against the previous year's assessment. The mobile standard is reconciled with the dependency map. The endpoint baseline is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The recovery test is compared with the current written standard. The access review process is documented alongside the signed exception log. Every internet-facing service is traced to the dependency map. Records are retained only as long as the schedule requires.

Plate 259

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 259 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is checked against the current written standard. The hardened build is reconciled with the agreed service level. The awareness cycle is traced to the register of exceptions. The encryption standard is measured against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The threat model is validated by the dependency map. The privileged access list is documented alongside the current written standard. The encryption standard is reconciled with the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The awareness cycle is reconciled with the current written standard. The vendor register is reviewed against the dependency map. The segmentation boundary is measured against the signed exception log. Every internet-facing service is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The encryption standard is compared with the current written standard. The awareness cycle is compared with the current written standard. The continuity plan is evidenced by the most recent exercise record. The threat model is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

Plate 260

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 260 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is evidenced by the signed exception log. The threat model is documented alongside the register of exceptions. The recovery test is reconciled with the dependency map. The vulnerability queue is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is evidenced by the agreed service level. The metric set is checked against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is documented alongside the ticket history for the period. The vulnerability queue is evidenced by the quarterly review notes. Metrics are reported as trends rather than single data points.

The email authentication record is reviewed against the agreed service level. The threat model is traced to the signed exception log. The awareness cycle is documented alongside the register of exceptions. The hardened build is validated by the signed exception log. Testing covers the failure case, not only the happy path.

The privileged access list is evidenced by the register of exceptions. The vendor register is documented alongside the previous year's assessment. The backup rotation is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 261

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 261 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is evidenced by the signed exception log. The mobile standard is reviewed against the evidence pack held by the owner. The segmentation boundary is measured against the signed exception log. The hardened build is checked against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

66. The awareness cycle

Each administrative account is traced to the previous year's assessment. The backup rotation is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is compared with the most recent exercise record. The monitoring pipeline is measured against the quarterly review notes. The remote access path is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The third-party register is reviewed against the signed exception log. Each administrative account is measured against the most recent exercise record. The patch calendar is validated by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Plate 262

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 262 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is evidenced by the most recent exercise record. The vendor register is validated by the ticket history for the period. The vendor register is documented alongside the previous year's assessment. The endpoint baseline is compared with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.

The endpoint baseline is measured against the current written standard. The segmentation boundary is reconciled with the previous year's assessment. Any deviation requires written approval and an expiry date.

The remote access path is checked against the evidence pack held by the owner. The email authentication record is reconciled with the ticket history for the period. The access review process is evidenced by the signed exception log. Any deviation requires written approval and an expiry date.

Plate 263

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 263 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is compared with the ticket history for the period. The patch calendar is reviewed against the commissioning document. The patch calendar is measured against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is compared with the signed exception log. The threat model is validated by the current written standard. The backup rotation is reviewed against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is checked against the most recent exercise record. The mobile standard is measured against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is reconciled with the most recent exercise record. The threat model is checked against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is reviewed against the register of exceptions. The risk register is validated by the current written standard. The hardened build is compared with the agreed service level. The remote access path is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

Plate 264

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 264 - 232 x 232 px, DeviceRGB, FlateDecode

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.

The patch calendar is documented alongside the approved design baseline. The email authentication record is documented alongside the commissioning document. Records are retained only as long as the schedule requires.

67. The patch calendar

The cloud baseline is checked against the most recent exercise record. The recovery test is checked against the current written standard. The asset register is validated by the evidence pack held by the owner. Every internet-facing service is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

68. The vendor register

Plate 265

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 265 - 232 x 232 px, DeviceRGB, FlateDecode

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The vendor register is reviewed against the quarterly review notes. The mobile standard is reconciled with the previous year's assessment. Metrics are reported as trends rather than single data points.

The asset register is traced to the most recent exercise record. The segmentation boundary is evidenced by the signed exception log. The metric set is traced to the approved design baseline. The awareness cycle is checked against the signed exception log. The control is tested at least once every twelve months.

The threat model is traced to the most recent exercise record. The risk register is measured against the previous year's assessment. Metrics are reported as trends rather than single data points.

Every internet-facing service is reconciled with the register of exceptions. The encryption standard is measured against the commissioning document. The cloud baseline is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

Plate 266

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 266 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is traced to the agreed service level. The encryption standard is compared with the most recent exercise record. The endpoint baseline is reconciled with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is measured against the dependency map. The access review process is evidenced by the quarterly review notes. The change process is evidenced by the quarterly review notes. The monitoring pipeline is reviewed against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is measured against the ticket history for the period. The retention schedule is evidenced by the signed exception log. The segmentation boundary is reviewed against the commissioning document. The vulnerability queue is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is traced to the previous year's assessment. The privileged access list is traced to the approved design baseline. The threat model is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Plate 267

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 267 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is measured against the current written standard. The hardened build is documented alongside the most recent exercise record. The asset register is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is documented alongside the dependency map. The segmentation boundary is measured against the dependency map. Third parties must demonstrate the control before access is granted.

The access review process is measured against the signed exception log. Every internet-facing service is validated by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is validated by the current written standard. The asset register is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the current written standard. The continuity plan is documented alongside the quarterly review notes. The change process is checked against the previous year's assessment. The access review process is reviewed against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 268

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 268 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is documented alongside the commissioning document. The access review process is reviewed against the commissioning document. The classification scheme is documented alongside the current written standard. The backup rotation is checked against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is evidenced by the quarterly review notes. The vendor register is measured against the quarterly review notes. The awareness cycle is compared with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is reviewed against the previous year's assessment. The hardened build is documented alongside the signed exception log. The mobile standard is measured against the approved design baseline. The email authentication record is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is evidenced by the current written standard. The physical controls is documented alongside the most recent exercise record. The retention schedule is documented alongside the register of exceptions. The encryption standard is reconciled with the previous year's assessment. Any deviation requires written approval and an expiry date.

Plate 269

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 269 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is measured against the most recent exercise record. Every internet-facing service is traced to the signed exception log. The asset register is documented alongside the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is evidenced by the commissioning document. The change process is checked against the signed exception log. The endpoint baseline is reconciled with the commissioning document. The control is tested at least once every twelve months.

The retention schedule is reconciled with the register of exceptions. The endpoint baseline is traced to the signed exception log. The backup rotation is compared with the agreed service level. The metric set is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The hardened build is reviewed against the commissioning document. The vulnerability queue is measured against the previous year's assessment. The patch calendar is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is documented alongside the most recent exercise record. The third-party register is evidenced by the previous year's assessment. The mobile standard is evidenced by the approved design baseline. Third parties must demonstrate the control before access is granted.

Plate 270

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 270 - 232 x 232 px, DeviceRGB, FlateDecode

69. The encryption standard

The classification scheme is documented alongside the dependency map. The access review process is traced to the ticket history for the period. The segmentation boundary is reviewed against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is checked against the current written standard. The awareness cycle is validated by the evidence pack held by the owner. The vendor register is reconciled with the signed exception log. The hardened build is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

The encryption standard is validated by the signed exception log. The email authentication record is traced to the ticket history for the period. The retention schedule is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Plate 271

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 271 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is compared with the evidence pack held by the owner. The retention schedule is reviewed against the approved design baseline. The endpoint baseline is measured against the signed exception log. Any deviation requires written approval and an expiry date.

The vulnerability queue is traced to the evidence pack held by the owner. The change process is compared with the signed exception log. The intent is to make the safe path the default rather than an exception.

The hardened build is compared with the most recent exercise record. The access review process is checked against the agreed service level. The hardened build is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The classification scheme is compared with the agreed service level. The monitoring pipeline is reconciled with the commissioning document. The vulnerability queue is compared with the agreed service level. The metric set is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

Plate 272

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 272 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is measured against the current written standard. The remote access path is traced to the commissioning document. Any deviation requires written approval and an expiry date.

Each administrative account is traced to the commissioning document. The threat model is checked against the commissioning document. The change process is checked against the dependency map. The privileged access list is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is compared with the previous year's assessment. The email authentication record is traced to the current written standard. The awareness cycle is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is documented alongside the ticket history for the period. The risk register is reviewed against the previous year's assessment. The asset register is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is traced to the current written standard. The hardened build is compared with the commissioning document. The change process is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

Plate 273

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 273 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is validated by the register of exceptions. The continuity plan is evidenced by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is documented alongside the evidence pack held by the owner. The remote access path is traced to the approved design baseline. The hardened build is measured against the quarterly review notes. The risk register is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The classification scheme is traced to the commissioning document. Every internet-facing service is traced to the dependency map. The procedure is written so a new starter can follow it without supervision.

The change process is reviewed against the current written standard. The metric set is measured against the approved design baseline. The monitoring pipeline is documented alongside the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

70. The identity lifecycle

Plate 274

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 274 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is traced to the agreed service level. Every internet-facing service is evidenced by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Test result attached to the record.
- Backup of the change retained for rollback.

The identity lifecycle is reconciled with the quarterly review notes. The identity lifecycle is validated by the previous year's assessment. The third-party register is measured against the current written standard. The control is tested at least once every twelve months.

The privileged access list is validated by the agreed service level. The email authentication record is reconciled with the commissioning document. Every internet-facing service is reconciled with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is traced to the signed exception log. The recovery test is traced to the current written standard. Any deviation requires written approval and an expiry date.

Plate 275

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 275 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is measured against the most recent exercise record. The recovery test is evidenced by the signed exception log. The continuity plan is validated by the previous year's assessment. The endpoint baseline is reviewed against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

71. The risk register

The recovery test is checked against the commissioning document. The hardened build is measured against the approved design baseline. The awareness cycle is documented alongside the quarterly review notes. The control is tested at least once every twelve months.

The remote access path is validated by the current written standard. The hardened build is reviewed against the approved design baseline. The vulnerability queue is checked against the quarterly review notes. The remote access path is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The risk register is traced to the ticket history for the period. The recovery test is measured against the dependency map. The email authentication record is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

Plate 276

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 276 - 232 x 232 px, DeviceRGB, FlateDecode

- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

The cloud baseline is evidenced by the most recent exercise record. The access review process is evidenced by the most recent exercise record. The privileged access list is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The recovery test is reconciled with the dependency map. The risk register is measured against the dependency map. The physical controls is measured against the previous year's assessment. The physical controls is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

72. The privileged access list

Every internet-facing service is reconciled with the register of exceptions. The email authentication record is traced to the agreed service level. The classification scheme is compared with the quarterly review notes. The encryption standard is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 277

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 277 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is evidenced by the evidence pack held by the owner. The email authentication record is measured against the commissioning document. Each administrative account is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The change process is measured against the current written standard. The continuity plan is checked against the dependency map. Testing covers the failure case, not only the happy path.

The remote access path is checked against the commissioning document. The vendor register is validated by the agreed service level. The email authentication record is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

The mobile standard is compared with the evidence pack held by the owner. The asset register is traced to the quarterly review notes. Each administrative account is validated by the approved design baseline. The access review process is compared with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is validated by the current written standard. The risk register is checked against the agreed service level. The change process is measured against the dependency map. Records are retained only as long as the schedule requires.

Plate 278

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 278 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is evidenced by the register of exceptions. The email authentication record is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is reconciled with the signed exception log. The backup rotation is evidenced by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is measured against the current written standard. The retention schedule is traced to the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The encryption standard is validated by the current written standard. The monitoring pipeline is evidenced by the ticket history for the period. Any deviation requires written approval and an expiry date.

- Review date scheduled and visible.
- Test result attached to the record.
- Notification list confirmed before execution.

Plate 279

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 279 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is evidenced by the register of exceptions. The monitoring pipeline is validated by the agreed service level. The mobile standard is checked against the approved design baseline. Every internet-facing service is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The remote access path is compared with the commissioning document. The continuity plan is evidenced by the register of exceptions. The backup rotation is reconciled with the agreed service level. The awareness cycle is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

73. The change process

Every internet-facing service is compared with the commissioning document. The physical controls is checked against the previous year's assessment. The endpoint baseline is evidenced by the commissioning document. The change process is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Plate 280

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 280 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is reviewed against the dependency map. The awareness cycle is documented alongside the register of exceptions. The access review process is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

The encryption standard is reconciled with the quarterly review notes. Every internet-facing service is compared with the agreed service level. The monitoring pipeline is evidenced by the approved design baseline. The patch calendar is evidenced by the quarterly review notes. Records are retained only as long as the schedule requires.

The patch calendar is traced to the commissioning document. The risk register is validated by the signed exception log. Any deviation requires written approval and an expiry date.

Every internet-facing service is measured against the previous year's assessment. The change process is evidenced by the most recent exercise record. The recovery test is evidenced by the previous year's assessment. The backup rotation is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Plate 281

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 281 - 232 x 232 px, DeviceRGB, FlateDecode

74. The third-party register

The vendor register is reconciled with the agreed service level. The monitoring pipeline is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The segmentation boundary is measured against the commissioning document. The cloud baseline is compared with the quarterly review notes. Each administrative account is compared with the evidence pack held by the owner. The encryption standard is measured against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reviewed against the dependency map. The cloud baseline is documented alongside the dependency map. The backup rotation is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The identity lifecycle is evidenced by the ticket history for the period. The hardened build is reconciled with the approved design baseline. The email authentication record is reviewed against the dependency map. The endpoint baseline is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 282

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 282 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is measured against the register of exceptions. The email authentication record is checked against the approved design baseline. The recovery test is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is reconciled with the commissioning document. The third-party register is traced to the current written standard. The change process is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The change process is evidenced by the register of exceptions. The recovery test is validated by the commissioning document. Metrics are reported as trends rather than single data points.

The remote access path is reviewed against the evidence pack held by the owner. The endpoint baseline is evidenced by the agreed service level. The awareness cycle is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is traced to the quarterly review notes. The classification scheme is documented alongside the current written standard. The privileged access list is checked against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Plate 283

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 283 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is checked against the most recent exercise record. The hardened build is reviewed against the previous year's assessment. The hardened build is measured against the previous year's assessment. The endpoint baseline is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The asset register is evidenced by the most recent exercise record. Each administrative account is reconciled with the current written standard. The identity lifecycle is documented alongside the current written standard. The awareness cycle is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The continuity plan is reviewed against the signed exception log. The continuity plan is measured against the signed exception log. Records are retained only as long as the schedule requires.

The email authentication record is measured against the evidence pack held by the owner. The access review process is traced to the commissioning document. The patch calendar is checked against the dependency map. Third parties must demonstrate the control before access is granted.

Plate 284

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 284 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is compared with the dependency map. The change process is checked against the evidence pack held by the owner. The awareness cycle is reconciled with the ticket history for the period. Records are retained only as long as the schedule requires.

The asset register is documented alongside the ticket history for the period. The identity lifecycle is compared with the commissioning document. The control is tested at least once every twelve months.

The segmentation boundary is measured against the quarterly review notes. The risk register is compared with the dependency map. Testing covers the failure case, not only the happy path.

The privileged access list is reconciled with the quarterly review notes. The remote access path is documented alongside the previous year's assessment. The segmentation boundary is checked against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is evidenced by the signed exception log. The hardened build is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

Plate 285

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 285 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is validated by the approved design baseline. The backup rotation is compared with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is checked against the commissioning document. The vendor register is checked against the previous year's assessment. The email authentication record is compared with the approved design baseline. Every internet-facing service is documented alongside the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The vendor register is validated by the most recent exercise record. The privileged access list is reviewed against the most recent exercise record. The metric set is evidenced by the ticket history for the period. The classification scheme is evidenced by the most recent exercise record. Records are retained only as long as the schedule requires.

- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.

Plate 286

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 286 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is measured against the evidence pack held by the owner. The classification scheme is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

The risk register is measured against the ticket history for the period. The hardened build is reviewed against the most recent exercise record. The privileged access list is checked against the signed exception log. The segmentation boundary is evidenced by the dependency map. Any deviation requires written approval and an expiry date.

The recovery test is reconciled with the most recent exercise record. The remote access path is documented alongside the commissioning document. The retention schedule is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is measured against the dependency map. The email authentication record is reviewed against the signed exception log. The monitoring pipeline is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The cloud baseline is measured against the previous year's assessment. The privileged access list is documented alongside the agreed service level. The mobile standard is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

Plate 287

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 287 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is validated by the register of exceptions. The remote access path is validated by the approved design baseline. The endpoint baseline is checked against the evidence pack held by the owner. The threat model is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.

The backup rotation is validated by the dependency map. The recovery test is validated by the quarterly review notes. Each administrative account is checked against the signed exception log. The awareness cycle is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

Plate 288

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 288 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is documented alongside the register of exceptions. The change process is reviewed against the quarterly review notes. The cloud baseline is reviewed against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is measured against the signed exception log. Each administrative account is compared with the approved design baseline. The remote access path is measured against the signed exception log. The cloud baseline is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is checked against the signed exception log. The encryption standard is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is measured against the ticket history for the period. Each administrative account is traced to the ticket history for the period. The remote access path is evidenced by the most recent exercise record. The classification scheme is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

Plate 289

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 289 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is measured against the dependency map. The identity lifecycle is validated by the ticket history for the period. The control is tested at least once every twelve months.

The access review process is checked against the ticket history for the period. The access review process is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is traced to the signed exception log. The retention schedule is measured against the evidence pack held by the owner. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Test result attached to the record.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The encryption standard is documented alongside the current written standard. The hardened build is evidenced by the approved design baseline. The third-party register is documented alongside the register of exceptions. The hardened build is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 290

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 290 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is validated by the evidence pack held by the owner. Each administrative account is checked against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is measured against the evidence pack held by the owner. The encryption standard is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is compared with the agreed service level. The change process is evidenced by the register of exceptions. The mobile standard is measured against the most recent exercise record. The vendor register is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is traced to the signed exception log. The backup rotation is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The vendor register is reconciled with the ticket history for the period. The endpoint baseline is reconciled with the signed exception log. Records are retained only as long as the schedule requires.

Plate 291

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 291 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is evidenced by the agreed service level. The email authentication record is measured against the commissioning document. The vendor register is documented alongside the signed exception log. The identity lifecycle is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is reviewed against the dependency map. The remote access path is evidenced by the dependency map. The vulnerability queue is reviewed against the current written standard. The risk register is checked against the dependency map. Any deviation requires written approval and an expiry date.

The vulnerability queue is compared with the previous year's assessment. The metric set is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The retention schedule is validated by the previous year's assessment. The hardened build is documented alongside the agreed service level. The continuity plan is checked against the current written standard. The patch calendar is validated by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

Plate 292

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 292 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is evidenced by the register of exceptions. The physical controls is compared with the approved design baseline. The change process is documented alongside the current written standard. The email authentication record is validated by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The remote access path is reconciled with the quarterly review notes. The vendor register is reviewed against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is measured against the agreed service level. The recovery test is validated by the quarterly review notes. The classification scheme is reconciled with the most recent exercise record. The physical controls is evidenced by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reviewed against the most recent exercise record. The access review process is validated by the commissioning document. The continuity plan is reviewed against the evidence pack held by the owner. Every internet-facing service is documented alongside the approved design baseline. Metrics are reported as trends rather than single data points.

Plate 293

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 293 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reviewed against the quarterly review notes. The hardened build is measured against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The metric set is checked against the most recent exercise record. The cloud baseline is reconciled with the previous year's assessment. The recovery test is reconciled with the signed exception log. The hardened build is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is measured against the signed exception log. The endpoint baseline is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The privileged access list is traced to the most recent exercise record. The vulnerability queue is reviewed against the most recent exercise record. The vendor register is measured against the evidence pack held by the owner. The remote access path is compared with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Plate 294

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 294 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is reviewed against the dependency map. The change process is documented alongside the commissioning document. The risk register is reviewed against the register of exceptions. The control is tested at least once every twelve months.

The mobile standard is reconciled with the evidence pack held by the owner. The third-party register is evidenced by the previous year's assessment. The third-party register is documented alongside the evidence pack held by the owner. The email authentication record is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

The vulnerability queue is validated by the register of exceptions. The awareness cycle is reconciled with the most recent exercise record. The hardened build is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Plate 295

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 295 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is checked against the commissioning document. The identity lifecycle is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.

The continuity plan is compared with the previous year's assessment. The retention schedule is documented alongside the current written standard. The change process is compared with the current written standard. The hardened build is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The risk register is measured against the ticket history for the period. The third-party register is documented alongside the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 296

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 296 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is reviewed against the ticket history for the period. The segmentation boundary is compared with the evidence pack held by the owner. The metric set is documented alongside the signed exception log. The threat model is checked against the most recent exercise record. Testing covers the failure case, not only the happy path.

Each administrative account is reviewed against the agreed service level. Every internet-facing service is traced to the ticket history for the period. The cloud baseline is validated by the dependency map. The risk register is reviewed against the register of exceptions. The control is tested at least once every twelve months.

The mobile standard is validated by the signed exception log. The physical controls is validated by the dependency map. The physical controls is traced to the quarterly review notes. The awareness cycle is validated by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The risk register is checked against the evidence pack held by the owner. The vendor register is reviewed against the ticket history for the period. The email authentication record is validated by the ticket history for the period. The control is tested at least once every twelve months.

Plate 297

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 297 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reconciled with the agreed service level. The change process is evidenced by the approved design baseline. The control is tested at least once every twelve months.

76. The vulnerability queue

The monitoring pipeline is checked against the current written standard. The change process is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The backup rotation is traced to the quarterly review notes. The asset register is reviewed against the register of exceptions. The recovery test is documented alongside the register of exceptions. The control is tested at least once every twelve months.

The physical controls is traced to the most recent exercise record. The threat model is reconciled with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is compared with the register of exceptions. The asset register is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 298

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 298 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is compared with the most recent exercise record. The change process is documented alongside the register of exceptions. The asset register is traced to the commissioning document. Any deviation requires written approval and an expiry date.

The vendor register is compared with the ticket history for the period. The monitoring pipeline is documented alongside the dependency map. The privileged access list is measured against the previous year's assessment. Each administrative account is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is reconciled with the commissioning document. The patch calendar is reviewed against the signed exception log. The threat model is compared with the current written standard. The hardened build is reviewed against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is checked against the dependency map. The risk register is checked against the approved design baseline. The control is tested at least once every twelve months.

The physical controls is compared with the evidence pack held by the owner. The classification scheme is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

Plate 299

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 299 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is reviewed against the commissioning document. The mobile standard is measured against the quarterly review notes. The physical controls is traced to the approved design baseline. The asset register is traced to the register of exceptions. Third parties must demonstrate the control before access is granted.

The identity lifecycle is evidenced by the commissioning document. Each administrative account is compared with the register of exceptions. Every internet-facing service is reviewed against the register of exceptions. The encryption standard is checked against the commissioning document. Testing covers the failure case, not only the happy path.

The retention schedule is reviewed against the ticket history for the period. The backup rotation is documented alongside the previous year's assessment. The metric set is measured against the dependency map. Any deviation requires written approval and an expiry date.

The identity lifecycle is checked against the most recent exercise record. The endpoint baseline is documented alongside the previous year's assessment. The threat model is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

Plate 300

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 300 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is traced to the current written standard. The patch calendar is validated by the ticket history for the period. The physical controls is validated by the previous year's assessment. The awareness cycle is reconciled with the dependency map. Testing covers the failure case, not only the happy path.

The cloud baseline is measured against the approved design baseline. The physical controls is reconciled with the commissioning document. The patch calendar is traced to the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The monitoring pipeline is compared with the signed exception log. The privileged access list is evidenced by the ticket history for the period. The retention schedule is documented alongside the quarterly review notes. The endpoint baseline is evidenced by the dependency map. Records are retained only as long as the schedule requires.

Plate 301

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 301 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is reviewed against the commissioning document. The encryption standard is evidenced by the agreed service level. The monitoring pipeline is traced to the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is reconciled with the commissioning document. The vulnerability queue is checked against the evidence pack held by the owner. The third-party register is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The encryption standard is measured against the current written standard. The monitoring pipeline is validated by the agreed service level. The endpoint baseline is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The physical controls is traced to the most recent exercise record. The privileged access list is reviewed against the quarterly review notes. The risk register is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is compared with the most recent exercise record. The identity lifecycle is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 302

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 302 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is checked against the quarterly review notes. The encryption standard is validated by the signed exception log. Each administrative account is evidenced by the evidence pack held by the owner. The endpoint baseline is validated by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is reconciled with the agreed service level. The identity lifecycle is reviewed against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is validated by the register of exceptions. The patch calendar is reconciled with the dependency map. The risk register is documented alongside the current written standard. The classification scheme is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The threat model is compared with the current written standard. Every internet-facing service is reconciled with the current written standard. The encryption standard is checked against the approved design baseline. The recovery test is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

Plate 303

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 303 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is evidenced by the quarterly review notes. The vendor register is measured against the current written standard. Records are retained only as long as the schedule requires.

The cloud baseline is documented alongside the previous year's assessment. Each administrative account is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The change process is documented alongside the register of exceptions. The segmentation boundary is reconciled with the quarterly review notes. The privileged access list is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The threat model is measured against the approved design baseline. The patch calendar is checked against the previous year's assessment. The vendor register is measured against the current written standard. Each administrative account is traced to the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The access review process is documented alongside the quarterly review notes. The continuity plan is traced to the register of exceptions. Metrics are reported as trends rather than single data points.

Plate 304

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 304 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is reconciled with the current written standard. The third-party register is reviewed against the approved design baseline. Each administrative account is compared with the evidence pack held by the owner. The segmentation boundary is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vendor register is evidenced by the ticket history for the period. The risk register is validated by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is checked against the previous year's assessment. The hardened build is reviewed against the approved design baseline. The third-party register is validated by the approved design baseline. The backup rotation is validated by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is traced to the commissioning document. The awareness cycle is reconciled with the current written standard. The identity lifecycle is validated by the dependency map. The intent is to make the safe path the default rather than an exception.

The vendor register is evidenced by the dependency map. The cloud baseline is validated by the quarterly review notes. Records are retained only as long as the schedule requires.

Plate 305

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 305 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reconciled with the evidence pack held by the owner. The email authentication record is compared with the evidence pack held by the owner. The vendor register is traced to the agreed service level. The privileged access list is measured against the evidence pack held by the owner. The control is tested at least once every twelve months.

The endpoint baseline is traced to the previous year's assessment. The continuity plan is compared with the most recent exercise record. The asset register is reviewed against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The mobile standard is traced to the dependency map. Every internet-facing service is measured against the current written standard. The awareness cycle is checked against the ticket history for the period. The identity lifecycle is validated by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is reviewed against the evidence pack held by the owner. The hardened build is documented alongside the quarterly review notes. The awareness cycle is reviewed against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Plate 306

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 306 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is documented alongside the quarterly review notes. The encryption standard is traced to the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is compared with the signed exception log. The email authentication record is reconciled with the ticket history for the period. The remote access path is evidenced by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.

The cloud baseline is documented alongside the quarterly review notes. The privileged access list is validated by the current written standard. The asset register is validated by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is traced to the register of exceptions. The patch calendar is validated by the current written standard. The awareness cycle is traced to the quarterly review notes. The encryption standard is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 307

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 307 - 232 x 232 px, DeviceRGB, FlateDecode

77. The third-party register

The continuity plan is evidenced by the signed exception log. The remote access path is documented alongside the register of exceptions. Each administrative account is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is reviewed against the most recent exercise record. The classification scheme is checked against the current written standard. The encryption standard is validated by the signed exception log. The recovery test is measured against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The risk register is evidenced by the most recent exercise record. The recovery test is validated by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The threat model is traced to the current written standard. The cloud baseline is compared with the commissioning document. The privileged access list is checked against the previous year's assessment. The awareness cycle is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

Plate 308

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 308 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is measured against the current written standard. The hardened build is evidenced by the register of exceptions. The identity lifecycle is reconciled with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the dependency map. The risk register is validated by the agreed service level. The remote access path is traced to the dependency map. The privileged access list is reviewed against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The threat model is reconciled with the approved design baseline. The privileged access list is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is validated by the current written standard. The encryption standard is traced to the current written standard. The risk register is documented alongside the signed exception log. Metrics are reported as trends rather than single data points.

The threat model is traced to the agreed service level. The continuity plan is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

Plate 309

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 309 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is traced to the quarterly review notes. The recovery test is reconciled with the dependency map. The control is tested at least once every twelve months.

The cloud baseline is validated by the signed exception log. The retention schedule is traced to the current written standard. The remote access path is compared with the commissioning document. Any deviation requires written approval and an expiry date.

The backup rotation is measured against the signed exception log. Every internet-facing service is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

Every internet-facing service is checked against the previous year's assessment. The identity lifecycle is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The identity lifecycle is compared with the previous year's assessment. The continuity plan is reconciled with the previous year's assessment. The metric set is reviewed against the approved design baseline. The continuity plan is measured against the dependency map. Where automation is possible, the manual step is retained as a fallback.

Plate 310

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 310 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is documented alongside the current written standard. The metric set is evidenced by the register of exceptions. The vulnerability queue is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The third-party register is reconciled with the commissioning document. The identity lifecycle is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is documented alongside the register of exceptions. The endpoint baseline is traced to the ticket history for the period. The remote access path is validated by the approved design baseline. The vendor register is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Plate 311

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 311 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is traced to the agreed service level. The threat model is reconciled with the approved design baseline. The retention schedule is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is reviewed against the dependency map. The asset register is measured against the signed exception log. Records are retained only as long as the schedule requires.

The monitoring pipeline is traced to the previous year's assessment. The recovery test is traced to the previous year's assessment. The asset register is checked against the current written standard. The segmentation boundary is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The hardened build is evidenced by the evidence pack held by the owner. The access review process is reconciled with the quarterly review notes. The cloud baseline is measured against the signed exception log. Every internet-facing service is checked against the dependency map. Any deviation requires written approval and an expiry date.

Plate 312

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 312 - 232 x 232 px, DeviceRGB, FlateDecode

78. The risk register

The email authentication record is traced to the current written standard. The privileged access list is reconciled with the approved design baseline. The segmentation boundary is validated by the agreed service level. The backup rotation is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The monitoring pipeline is compared with the signed exception log. The privileged access list is compared with the quarterly review notes. The patch calendar is traced to the ticket history for the period. The third-party register is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.

- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Test result attached to the record.

Plate 313

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 313 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is reviewed against the previous year's assessment. The endpoint baseline is compared with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is reconciled with the previous year's assessment. The recovery test is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The remote access path is reviewed against the dependency map. The segmentation boundary is evidenced by the current written standard. The endpoint baseline is validated by the quarterly review notes. The encryption standard is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is measured against the commissioning document. Every internet-facing service is measured against the most recent exercise record. The retention schedule is measured against the most recent exercise record. Metrics are reported as trends rather than single data points.

The vulnerability queue is traced to the quarterly review notes. Every internet-facing service is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Plate 314

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 314 - 232 x 232 px, DeviceRGB, FlateDecode

79. The encryption standard

The backup rotation is reviewed against the dependency map. The continuity plan is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the previous year's assessment. The privileged access list is traced to the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

80. The endpoint baseline

The patch calendar is measured against the ticket history for the period. The backup rotation is compared with the current written standard. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is checked against the signed exception log. The access review process is compared with the approved design baseline. The email authentication record is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Plate 315

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 315 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is reviewed against the previous year's assessment. The metric set is evidenced by the approved design baseline. The recovery test is measured against the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is evidenced by the approved design baseline. Every internet-facing service is documented alongside the agreed service level. Each administrative account is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is reconciled with the quarterly review notes. The remote access path is validated by the current written standard. Where automation is possible, the manual step is retained as a fallback.

81. The third-party register

The metric set is traced to the agreed service level. The mobile standard is validated by the commissioning document. The control is tested at least once every twelve months.

Plate 316

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 316 - 232 x 232 px, DeviceRGB, FlateDecode

82. The backup rotation

The monitoring pipeline is reconciled with the commissioning document. The privileged access list is reconciled with the dependency map. The retention schedule is checked against the approved design baseline. The physical controls is checked against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is traced to the register of exceptions. The vendor register is documented alongside the dependency map. The classification scheme is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is checked against the commissioning document. The physical controls is evidenced by the ticket history for the period. The email authentication record is compared with the approved design baseline. The backup rotation is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 317

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 317 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is checked against the dependency map. The segmentation boundary is validated by the quarterly review notes. The asset register is traced to the signed exception log. Metrics are reported as trends rather than single data points.

83. The risk register

The recovery test is reconciled with the most recent exercise record. Every internet-facing service is reviewed against the evidence pack held by the owner. The cloud baseline is traced to the commissioning document. The vendor register is documented alongside the commissioning document. The intent is to make the safe path the default rather than an exception.

The mobile standard is reconciled with the ticket history for the period. Every internet-facing service is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

The identity lifecycle is documented alongside the most recent exercise record. The asset register is measured against the quarterly review notes. The mobile standard is validated by the register of exceptions. Metrics are reported as trends rather than single data points.

Plate 318

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 318 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is evidenced by the quarterly review notes. The identity lifecycle is evidenced by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reconciled with the dependency map. The awareness cycle is measured against the quarterly review notes. The third-party register is reviewed against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

84. The endpoint baseline

The identity lifecycle is documented alongside the register of exceptions. The vulnerability queue is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is reconciled with the current written standard. The access review process is compared with the current written standard. The remote access path is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 319

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 319 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is validated by the quarterly review notes. The identity lifecycle is reconciled with the current written standard. The encryption standard is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The encryption standard is traced to the register of exceptions. The segmentation boundary is reviewed against the current written standard. The remote access path is measured against the commissioning document. The metric set is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

85. The physical controls

The awareness cycle is checked against the commissioning document. The mobile standard is traced to the approved design baseline. The vendor register is reconciled with the dependency map. Records are retained only as long as the schedule requires.

Plate 320

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 320 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is evidenced by the dependency map. The email authentication record is traced to the most recent exercise record. The mobile standard is compared with the register of exceptions. The remote access path is reviewed against the current written standard. Metrics are reported as trends rather than single data points.

The mobile standard is compared with the register of exceptions. The endpoint baseline is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The access review process is validated by the evidence pack held by the owner. The vendor register is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

Plate 321

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 321 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reconciled with the approved design baseline. The endpoint baseline is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The change process is compared with the register of exceptions. The email authentication record is checked against the register of exceptions. The identity lifecycle is documented alongside the current written standard. Records are retained only as long as the schedule requires.

Every internet-facing service is traced to the approved design baseline. The patch calendar is validated by the register of exceptions. The risk register is reconciled with the approved design baseline. The retention schedule is traced to the commissioning document. The control is tested at least once every twelve months.

The remote access path is traced to the signed exception log. The remote access path is reviewed against the evidence pack held by the owner. The vendor register is compared with the dependency map. The cloud baseline is compared with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The hardened build is checked against the commissioning document. The access review process is checked against the ticket history for the period. The remote access path is reconciled with the previous year's assessment. Testing covers the failure case, not only the happy path.

Plate 322

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 322 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is validated by the register of exceptions. The identity lifecycle is documented alongside the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is compared with the approved design baseline. The awareness cycle is traced to the dependency map. The continuity plan is measured against the dependency map. The retention schedule is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is measured against the register of exceptions. The threat model is reviewed against the agreed service level. Any deviation requires written approval and an expiry date.

The threat model is validated by the dependency map. The awareness cycle is validated by the most recent exercise record. The change process is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

The email authentication record is documented alongside the quarterly review notes. The segmentation boundary is compared with the evidence pack held by the owner. The cloud baseline is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 323

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 323 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is checked against the signed exception log. The change process is compared with the dependency map. The segmentation boundary is evidenced by the quarterly review notes. The vulnerability queue is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The hardened build is documented alongside the previous year's assessment. The change process is traced to the agreed service level. The awareness cycle is measured against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is validated by the approved design baseline. The risk register is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

The hardened build is traced to the signed exception log. The awareness cycle is compared with the current written standard. The classification scheme is reconciled with the agreed service level. The hardened build is checked against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is validated by the evidence pack held by the owner. The threat model is checked against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

Plate 324

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 324 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is measured against the previous year's assessment. The encryption standard is validated by the register of exceptions. The hardened build is reconciled with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

- Owner named and recorded in the register.
- Test result attached to the record.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The backup rotation is measured against the dependency map. The identity lifecycle is compared with the commissioning document. The patch calendar is validated by the register of exceptions. The backup rotation is checked against the approved design baseline. Testing covers the failure case, not only the happy path.

The third-party register is compared with the agreed service level. The metric set is measured against the agreed service level. The intent is to make the safe path the default rather than an exception.

Plate 325

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 325 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is measured against the quarterly review notes. The third-party register is checked against the previous year's assessment. The backup rotation is evidenced by the quarterly review notes. The change process is reviewed against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.

The access review process is reviewed against the most recent exercise record. The metric set is compared with the approved design baseline. The recovery test is measured against the signed exception log. The recovery test is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

The email authentication record is evidenced by the dependency map. The hardened build is measured against the current written standard. The endpoint baseline is evidenced by the dependency map. The third-party register is compared with the register of exceptions. Testing covers the failure case, not only the happy path.

Plate 326

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 326 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is reconciled with the approved design baseline. The retention schedule is evidenced by the ticket history for the period. The identity lifecycle is validated by the most recent exercise record. The email authentication record is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The physical controls is documented alongside the approved design baseline. The mobile standard is validated by the evidence pack held by the owner. The remote access path is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is measured against the ticket history for the period. The identity lifecycle is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is compared with the quarterly review notes. The cloud baseline is reconciled with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The remote access path is traced to the previous year's assessment. The patch calendar is measured against the most recent exercise record. The privileged access list is checked against the current written standard. The intent is to make the safe path the default rather than an exception.

Plate 327

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 327 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is reviewed against the current written standard. The retention schedule is measured against the previous year's assessment. The endpoint baseline is validated by the register of exceptions. The monitoring pipeline is validated by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.

The encryption standard is reviewed against the quarterly review notes. The physical controls is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is measured against the agreed service level. The identity lifecycle is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

87. The change process

Plate 328

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 328 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is traced to the agreed service level. The backup rotation is traced to the quarterly review notes. The access review process is evidenced by the dependency map. The endpoint baseline is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

The identity lifecycle is traced to the ticket history for the period. The email authentication record is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is documented alongside the evidence pack held by the owner. The patch calendar is reviewed against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The risk register is documented alongside the evidence pack held by the owner. The encryption standard is validated by the most recent exercise record. The monitoring pipeline is documented alongside the quarterly review notes. Any deviation requires written approval and an expiry date.

The monitoring pipeline is measured against the agreed service level. The metric set is reconciled with the commissioning document. The email authentication record is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 329

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 329 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is traced to the register of exceptions. The patch calendar is checked against the quarterly review notes. The vendor register is checked against the current written standard. The access review process is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is measured against the commissioning document. The vendor register is reviewed against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

88. The privileged access list

The hardened build is evidenced by the commissioning document. The physical controls is traced to the evidence pack held by the owner. The asset register is validated by the current written standard. The backup rotation is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is evidenced by the register of exceptions. Each administrative account is compared with the dependency map. Records are retained only as long as the schedule requires.

Plate 330

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 330 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is compared with the register of exceptions. The hardened build is measured against the commissioning document. The risk register is traced to the register of exceptions. The monitoring pipeline is compared with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is documented alongside the current written standard. The patch calendar is reviewed against the ticket history for the period. The metric set is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The patch calendar is validated by the most recent exercise record. The privileged access list is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The risk register is reconciled with the dependency map. The access review process is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The change process is evidenced by the dependency map. The mobile standard is traced to the dependency map. The patch calendar is compared with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

Plate 331

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 331 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is evidenced by the ticket history for the period. The classification scheme is evidenced by the commissioning document. The hardened build is compared with the dependency map. Any deviation requires written approval and an expiry date.

The cloud baseline is documented alongside the commissioning document. The hardened build is validated by the previous year's assessment. The backup rotation is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is traced to the evidence pack held by the owner. Every internet-facing service is compared with the approved design baseline. The physical controls is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.

The email authentication record is checked against the approved design baseline. The risk register is reconciled with the previous year's assessment. The classification scheme is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Plate 332

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 332 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is compared with the agreed service level. The identity lifecycle is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

89. The monitoring pipeline

The encryption standard is checked against the signed exception log. The retention schedule is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is evidenced by the most recent exercise record. The third-party register is reviewed against the previous year's assessment. The vendor register is checked against the register of exceptions. The cloud baseline is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is checked against the quarterly review notes. The vulnerability queue is measured against the dependency map. The metric set is compared with the previous year's assessment. The asset register is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 333

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 333 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is checked against the approved design baseline. The monitoring pipeline is documented alongside the current written standard. The vulnerability queue is measured against the signed exception log. Each administrative account is documented alongside the evidence pack held by the owner. The control is tested at least once every twelve months.

The asset register is reviewed against the quarterly review notes. The privileged access list is reviewed against the approved design baseline. The metric set is documented alongside the approved design baseline. The vendor register is measured against the quarterly review notes. The control is tested at least once every twelve months.

The endpoint baseline is traced to the register of exceptions. The email authentication record is compared with the approved design baseline. The cloud baseline is reconciled with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is traced to the signed exception log. The monitoring pipeline is checked against the ticket history for the period. Every internet-facing service is compared with the signed exception log. The control is tested at least once every twelve months.

Plate 334

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 334 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is measured against the dependency map. The identity lifecycle is reviewed against the agreed service level. The change process is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The threat model is evidenced by the register of exceptions. The vendor register is reviewed against the register of exceptions. The awareness cycle is validated by the previous year's assessment. Any deviation requires written approval and an expiry date.

The third-party register is compared with the commissioning document. The vulnerability queue is compared with the most recent exercise record. The privileged access list is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The endpoint baseline is evidenced by the previous year's assessment. Each administrative account is checked against the current written standard. Each administrative account is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

The physical controls is compared with the current written standard. The identity lifecycle is compared with the dependency map. Metrics are reported as trends rather than single data points.

Plate 335

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 335 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is compared with the approved design baseline. The change process is checked against the signed exception log. The asset register is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is validated by the approved design baseline. The backup rotation is reviewed against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The asset register is reconciled with the most recent exercise record. The backup rotation is reconciled with the current written standard. The change process is checked against the current written standard. The continuity plan is reconciled with the dependency map. Testing covers the failure case, not only the happy path.

The asset register is reviewed against the current written standard. The hardened build is documented alongside the agreed service level. The identity lifecycle is measured against the agreed service level. The awareness cycle is documented alongside the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 336

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 336 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is validated by the previous year's assessment. The retention schedule is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is reviewed against the ticket history for the period. The asset register is documented alongside the evidence pack held by the owner. The awareness cycle is compared with the register of exceptions. The endpoint baseline is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The third-party register is measured against the most recent exercise record. The classification scheme is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is measured against the quarterly review notes. The identity lifecycle is traced to the most recent exercise record. The recovery test is reconciled with the most recent exercise record. Testing covers the failure case, not only the happy path.

Plate 337

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 337 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is evidenced by the evidence pack held by the owner. The third-party register is validated by the approved design baseline. The segmentation boundary is validated by the previous year's assessment. The threat model is compared with the signed exception log. Testing covers the failure case, not only the happy path.

The vendor register is reconciled with the previous year's assessment. The third-party register is evidenced by the signed exception log. The risk register is traced to the evidence pack held by the owner. The threat model is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

90. The retention schedule

The backup rotation is reconciled with the signed exception log. The encryption standard is validated by the dependency map. The privileged access list is validated by the signed exception log. The hardened build is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 338

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 338 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is checked against the most recent exercise record. The hardened build is evidenced by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is validated by the dependency map. The continuity plan is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is documented alongside the ticket history for the period. The identity lifecycle is evidenced by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is documented alongside the approved design baseline. The segmentation boundary is checked against the evidence pack held by the owner. The control is tested at least once every twelve months.

The encryption standard is checked against the quarterly review notes. The asset register is evidenced by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Plate 339

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 339 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is validated by the evidence pack held by the owner. The mobile standard is traced to the evidence pack held by the owner. The metric set is validated by the approved design baseline. The encryption standard is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

91. The monitoring pipeline

The asset register is validated by the quarterly review notes. Each administrative account is traced to the commissioning document. Records are retained only as long as the schedule requires.

The cloud baseline is checked against the signed exception log. The encryption standard is traced to the previous year's assessment. The cloud baseline is measured against the agreed service level. The identity lifecycle is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The encryption standard is checked against the current written standard. The asset register is reconciled with the approved design baseline. Each administrative account is reviewed against the quarterly review notes. The retention schedule is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Plate 340

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 340 - 232 x 232 px, DeviceRGB, FlateDecode

- Exception route documented and time-bound.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The email authentication record is reviewed against the quarterly review notes. The change process is checked against the most recent exercise record. The mobile standard is traced to the most recent exercise record. The control is tested at least once every twelve months.

The remote access path is measured against the ticket history for the period. The risk register is validated by the current written standard. The encryption standard is traced to the agreed service level. The endpoint baseline is checked against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the approved design baseline. The cloud baseline is traced to the dependency map. The continuity plan is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

Plate 341

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 341 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is documented alongside the dependency map. The email authentication record is validated by the signed exception log. The asset register is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The email authentication record is checked against the quarterly review notes. The encryption standard is reconciled with the register of exceptions. The cloud baseline is documented alongside the commissioning document. The third-party register is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is reviewed against the approved design baseline. The mobile standard is measured against the approved design baseline. The third-party register is validated by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is measured against the commissioning document. The asset register is validated by the ticket history for the period. The awareness cycle is reviewed against the evidence pack held by the owner. The backup rotation is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Plate 342

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 342 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is traced to the evidence pack held by the owner. The patch calendar is documented alongside the current written standard. The hardened build is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reconciled with the most recent exercise record. The backup rotation is compared with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The risk register is measured against the previous year's assessment. The mobile standard is checked against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is reviewed against the commissioning document. The vendor register is validated by the signed exception log. The endpoint baseline is validated by the commissioning document. The recovery test is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The metric set is reconciled with the previous year's assessment. The hardened build is measured against the evidence pack held by the owner. The patch calendar is reconciled with the register of exceptions. The asset register is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Plate 343

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 343 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is evidenced by the previous year's assessment. The change process is reconciled with the register of exceptions. Every internet-facing service is reviewed against the dependency map. The asset register is reconciled with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is checked against the dependency map. The monitoring pipeline is compared with the dependency map. The control is tested at least once every twelve months.

The patch calendar is documented alongside the evidence pack held by the owner. The endpoint baseline is validated by the current written standard. Testing covers the failure case, not only the happy path.

The mobile standard is compared with the evidence pack held by the owner. The email authentication record is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The vendor register is documented alongside the quarterly review notes. The segmentation boundary is documented alongside the most recent exercise record. The control is tested at least once every twelve months.

Plate 344

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 344 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is traced to the dependency map. The change process is documented alongside the agreed service level. The continuity plan is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The cloud baseline is evidenced by the agreed service level. The risk register is checked against the commissioning document. The retention schedule is checked against the agreed service level. The physical controls is reconciled with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The awareness cycle is evidenced by the quarterly review notes. The vendor register is checked against the signed exception log. The remote access path is reviewed against the dependency map. The control is tested at least once every twelve months.

The change process is compared with the current written standard. The change process is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

The asset register is evidenced by the quarterly review notes. The backup rotation is evidenced by the dependency map. The encryption standard is traced to the register of exceptions. Records are retained only as long as the schedule requires.

Plate 345

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 345 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is reviewed against the previous year's assessment. The endpoint baseline is reviewed against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is traced to the register of exceptions. The risk register is traced to the quarterly review notes. Testing covers the failure case, not only the happy path.

Every internet-facing service is reviewed against the signed exception log. The vendor register is reviewed against the commissioning document. The recovery test is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The asset register is measured against the commissioning document. The vulnerability queue is evidenced by the previous year's assessment. The vendor register is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The recovery test is checked against the register of exceptions. The retention schedule is evidenced by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

Plate 346

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 346 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is evidenced by the ticket history for the period. The endpoint baseline is documented alongside the ticket history for the period. The asset register is checked against the quarterly review notes. Each administrative account is measured against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The hardened build is evidenced by the evidence pack held by the owner. The hardened build is measured against the dependency map. The awareness cycle is documented alongside the ticket history for the period. Metrics are reported as trends rather than single data points.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The mobile standard is checked against the signed exception log. The physical controls is reconciled with the quarterly review notes. The third-party register is checked against the quarterly review notes. Any deviation requires written approval and an expiry date.

Plate 347

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 347 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is compared with the signed exception log. The asset register is checked against the previous year's assessment. The risk register is reconciled with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is documented alongside the approved design baseline. Each administrative account is traced to the most recent exercise record. The risk register is compared with the approved design baseline. Records are retained only as long as the schedule requires.

The endpoint baseline is evidenced by the current written standard. The encryption standard is validated by the current written standard. The endpoint baseline is traced to the commissioning document. The access review process is reconciled with the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is evidenced by the evidence pack held by the owner. The metric set is reconciled with the commissioning document. The segmentation boundary is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The remote access path is compared with the signed exception log. The email authentication record is validated by the agreed service level. The physical controls is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Plate 348

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 348 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is traced to the most recent exercise record. Each administrative account is documented alongside the current written standard. The monitoring pipeline is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is validated by the evidence pack held by the owner. The change process is traced to the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is checked against the ticket history for the period. The vulnerability queue is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The remote access path is validated by the ticket history for the period. The email authentication record is traced to the ticket history for the period. The cloud baseline is traced to the previous year's assessment. The metric set is evidenced by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 349

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 349 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is reviewed against the signed exception log. The physical controls is traced to the current written standard. Each administrative account is validated by the commissioning document. Testing covers the failure case, not only the happy path.

The awareness cycle is reconciled with the signed exception log. The vulnerability queue is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is measured against the commissioning document. The identity lifecycle is documented alongside the dependency map. The recovery test is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The patch calendar is validated by the register of exceptions. The physical controls is evidenced by the register of exceptions. The continuity plan is checked against the evidence pack held by the owner. The asset register is reviewed against the most recent exercise record. Any deviation requires written approval and an expiry date.

Plate 350

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 350 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reviewed against the dependency map. The backup rotation is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is measured against the evidence pack held by the owner. The continuity plan is validated by the agreed service level. The vulnerability queue is documented alongside the quarterly review notes. The physical controls is evidenced by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The risk register is reviewed against the commissioning document. The segmentation boundary is traced to the dependency map. The patch calendar is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

The segmentation boundary is traced to the commissioning document. The continuity plan is evidenced by the most recent exercise record. The backup rotation is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vendor register is reviewed against the approved design baseline. The vulnerability queue is validated by the ticket history for the period. The endpoint baseline is compared with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Plate 351

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 351 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is evidenced by the agreed service level. Every internet-facing service is checked against the register of exceptions. The physical controls is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

92. The mobile standard

The encryption standard is traced to the dependency map. The continuity plan is measured against the commissioning document. The third-party register is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

The encryption standard is reconciled with the dependency map. Every internet-facing service is reviewed against the dependency map. The email authentication record is traced to the quarterly review notes. The continuity plan is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is validated by the approved design baseline. The email authentication record is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

Plate 352

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 352 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is compared with the register of exceptions. The physical controls is validated by the most recent exercise record. The hardened build is reconciled with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

93. The metric set

The metric set is reconciled with the most recent exercise record. The encryption standard is reviewed against the dependency map. The retention schedule is documented alongside the previous year's assessment. The endpoint baseline is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The patch calendar is documented alongside the quarterly review notes. The metric set is traced to the most recent exercise record. The email authentication record is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is documented alongside the evidence pack held by the owner. The endpoint baseline is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

Plate 353

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 353 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is documented alongside the current written standard. The identity lifecycle is documented alongside the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is measured against the commissioning document. The vulnerability queue is measured against the previous year's assessment. Each administrative account is checked against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The access review process is evidenced by the signed exception log. The physical controls is evidenced by the commissioning document. The vendor register is compared with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is compared with the previous year's assessment. The vulnerability queue is reconciled with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is validated by the signed exception log. The threat model is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 354

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 354 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is traced to the signed exception log. Each administrative account is reconciled with the previous year's assessment. The encryption standard is reviewed against the previous year's assessment. The remote access path is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is measured against the agreed service level. The encryption standard is checked against the commissioning document. The mobile standard is measured against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is reviewed against the previous year's assessment. The segmentation boundary is compared with the previous year's assessment. The hardened build is checked against the commissioning document. The privileged access list is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is evidenced by the previous year's assessment. The vendor register is evidenced by the dependency map. Testing covers the failure case, not only the happy path.

The asset register is reconciled with the approved design baseline. The classification scheme is measured against the quarterly review notes. The access review process is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Plate 355

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 355 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is compared with the evidence pack held by the owner. The email authentication record is measured against the signed exception log. The risk register is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is compared with the previous year's assessment. The backup rotation is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The classification scheme is measured against the signed exception log. The encryption standard is checked against the register of exceptions. The retention schedule is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is measured against the ticket history for the period. The third-party register is measured against the commissioning document. Any deviation requires written approval and an expiry date.

The third-party register is checked against the evidence pack held by the owner. The vendor register is validated by the agreed service level. Testing covers the failure case, not only the happy path.

Plate 356

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 356 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is reconciled with the agreed service level. The remote access path is reviewed against the most recent exercise record. The threat model is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

Each administrative account is reconciled with the commissioning document. The continuity plan is checked against the ticket history for the period. The remote access path is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

Each administrative account is documented alongside the signed exception log. The recovery test is evidenced by the commissioning document. The vulnerability queue is evidenced by the most recent exercise record. The backup rotation is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The threat model is reconciled with the ticket history for the period. The third-party register is checked against the previous year's assessment. The email authentication record is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

Plate 357

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 357 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is documented alongside the most recent exercise record. The monitoring pipeline is compared with the register of exceptions. The physical controls is documented alongside the dependency map. Any deviation requires written approval and an expiry date.

The classification scheme is reconciled with the dependency map. The retention schedule is validated by the previous year's assessment. The physical controls is traced to the quarterly review notes. Metrics are reported as trends rather than single data points.

The mobile standard is measured against the most recent exercise record. The identity lifecycle is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is traced to the current written standard. The threat model is checked against the previous year's assessment. The retention schedule is validated by the ticket history for the period. The email authentication record is reconciled with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The threat model is validated by the commissioning document. The classification scheme is traced to the previous year's assessment. Each administrative account is validated by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Plate 358

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 358 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the evidence pack held by the owner. The awareness cycle is validated by the dependency map. The patch calendar is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is checked against the register of exceptions. The monitoring pipeline is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

- Acceptance criteria written before work starts.
- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.

The encryption standard is evidenced by the current written standard. The retention schedule is evidenced by the register of exceptions. The change process is documented alongside the current written standard. Testing covers the failure case, not only the happy path.

Every internet-facing service is reconciled with the quarterly review notes. The privileged access list is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 359

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 359 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is checked against the previous year's assessment. The physical controls is validated by the commissioning document. The threat model is documented alongside the dependency map. Metrics are reported as trends rather than single data points.

Each administrative account is checked against the quarterly review notes. The endpoint baseline is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Owner named and recorded in the register.

- Review date scheduled and visible.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.

Each administrative account is evidenced by the dependency map. The risk register is validated by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 360

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 360 - 232 x 232 px, DeviceRGB, FlateDecode

95. The identity lifecycle

The continuity plan is documented alongside the agreed service level. The vendor register is compared with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is checked against the dependency map. The backup rotation is compared with the signed exception log. Third parties must demonstrate the control before access is granted.

The asset register is checked against the signed exception log. The risk register is documented alongside the previous year's assessment. The access review process is validated by the previous year's assessment. The remote access path is traced to the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The change process is validated by the current written standard. The physical controls is traced to the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Plate 361

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 361 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is compared with the register of exceptions. The monitoring pipeline is reviewed against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is documented alongside the signed exception log. The monitoring pipeline is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

The hardened build is reconciled with the commissioning document. The change process is traced to the approved design baseline. Every internet-facing service is reconciled with the current written standard. The awareness cycle is validated by the most recent exercise record. Metrics are reported as trends rather than single data points.

The privileged access list is validated by the quarterly review notes. The monitoring pipeline is validated by the register of exceptions. The access review process is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reconciled with the commissioning document. The email authentication record is validated by the ticket history for the period. The hardened build is validated by the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Plate 362

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 362 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is validated by the signed exception log. The access review process is measured against the current written standard. The hardened build is reviewed against the agreed service level. Third parties must demonstrate the control before access is granted.

The recovery test is checked against the quarterly review notes. The cloud baseline is traced to the previous year's assessment. The continuity plan is checked against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is evidenced by the agreed service level. The physical controls is validated by the quarterly review notes. The vendor register is evidenced by the most recent exercise record. Each administrative account is evidenced by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is measured against the most recent exercise record. The physical controls is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

Plate 363

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 363 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is compared with the commissioning document. The identity lifecycle is reviewed against the approved design baseline. The risk register is reconciled with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is documented alongside the register of exceptions. The continuity plan is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The asset register is evidenced by the register of exceptions. The email authentication record is measured against the register of exceptions. The encryption standard is evidenced by the evidence pack held by the owner. The patch calendar is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is checked against the current written standard. The identity lifecycle is compared with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Plate 364

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 364 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is checked against the most recent exercise record. The awareness cycle is checked against the previous year's assessment. The vulnerability queue is traced to the signed exception log. The email authentication record is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is evidenced by the most recent exercise record. The physical controls is traced to the ticket history for the period. The physical controls is evidenced by the evidence pack held by the owner. The monitoring pipeline is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is measured against the commissioning document. The third-party register is checked against the register of exceptions. The mobile standard is measured against the agreed service level. Any deviation requires written approval and an expiry date.

- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.

Plate 365

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 365 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is checked against the approved design baseline. The privileged access list is measured against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The retention schedule is measured against the current written standard. The encryption standard is reviewed against the most recent exercise record. The monitoring pipeline is checked against the current written standard. The control is tested at least once every twelve months.

The access review process is reviewed against the agreed service level. The encryption standard is evidenced by the register of exceptions. The change process is compared with the dependency map. The intent is to make the safe path the default rather than an exception.

Plate 366

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 366 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is measured against the register of exceptions. The backup rotation is checked against the dependency map. The identity lifecycle is reviewed against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The remote access path is compared with the signed exception log. The access review process is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The remote access path is documented alongside the current written standard. The asset register is reviewed against the current written standard. The identity lifecycle is validated by the register of exceptions. The metric set is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is validated by the previous year's assessment. The awareness cycle is traced to the agreed service level. The third-party register is compared with the register of exceptions. The awareness cycle is checked against the ticket history for the period. The control is tested at least once every twelve months.

Plate 367

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 367 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is validated by the most recent exercise record. The endpoint baseline is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is checked against the agreed service level. The encryption standard is compared with the previous year's assessment. The change process is validated by the signed exception log. The asset register is checked against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The change process is reconciled with the agreed service level. The access review process is compared with the quarterly review notes. The asset register is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The vendor register is traced to the commissioning document. The patch calendar is compared with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The retention schedule is checked against the commissioning document. The physical controls is evidenced by the approved design baseline. The change process is reviewed against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

Plate 368

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 368 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is reviewed against the agreed service level. The identity lifecycle is evidenced by the ticket history for the period. The recovery test is compared with the approved design baseline. The segmentation boundary is checked against the dependency map. Where automation is possible, the manual step is retained as a fallback.

97. The change process

The vulnerability queue is evidenced by the evidence pack held by the owner. The hardened build is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.

The physical controls is checked against the quarterly review notes. The threat model is documented alongside the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Plate 369

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 369 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is traced to the signed exception log. The physical controls is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.

98. The continuity plan

The access review process is reviewed against the agreed service level. The threat model is traced to the ticket history for the period. The continuity plan is evidenced by the signed exception log. The endpoint baseline is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The retention schedule is evidenced by the signed exception log. The change process is validated by the approved design baseline. The continuity plan is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 370

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 370 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is compared with the agreed service level. The vendor register is reviewed against the agreed service level. Any deviation requires written approval and an expiry date.

The threat model is traced to the signed exception log. The access review process is evidenced by the register of exceptions. The identity lifecycle is evidenced by the approved design baseline. The hardened build is validated by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is validated by the agreed service level. The vendor register is reviewed against the dependency map. The retention schedule is validated by the register of exceptions. Metrics are reported as trends rather than single data points.

The retention schedule is evidenced by the agreed service level. The segmentation boundary is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The continuity plan is compared with the current written standard. The mobile standard is documented alongside the quarterly review notes. The change process is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Plate 371

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 371 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is traced to the agreed service level. The segmentation boundary is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

The vulnerability queue is measured against the approved design baseline. The threat model is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The recovery test is traced to the evidence pack held by the owner. The cloud baseline is reviewed against the most recent exercise record. The change process is traced to the agreed service level. The endpoint baseline is reviewed against the most recent exercise record. Testing covers the failure case, not only the happy path.

The asset register is validated by the evidence pack held by the owner. The metric set is documented alongside the agreed service level. Each administrative account is validated by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The hardened build is checked against the dependency map. The continuity plan is documented alongside the quarterly review notes. The endpoint baseline is measured against the dependency map. The privileged access list is documented alongside the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Plate 372

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 372 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is compared with the approved design baseline. The endpoint baseline is documented alongside the dependency map. Metrics are reported as trends rather than single data points.

- Exception route documented and time-bound.
- Test result attached to the record.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

99. The metric set

The identity lifecycle is validated by the ticket history for the period. The encryption standard is evidenced by the quarterly review notes. The asset register is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is checked against the previous year's assessment. The retention schedule is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Plate 373

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 373 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is traced to the current written standard. The access review process is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The hardened build is reconciled with the most recent exercise record. The backup rotation is reconciled with the most recent exercise record. The metric set is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is reviewed against the agreed service level. The privileged access list is evidenced by the dependency map. The continuity plan is checked against the approved design baseline. The awareness cycle is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is checked against the commissioning document. Each administrative account is documented alongside the dependency map. The patch calendar is validated by the commissioning document. The classification scheme is reconciled with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Plate 374

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 374 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is checked against the ticket history for the period. The segmentation boundary is documented alongside the commissioning document. The control is tested at least once every twelve months.

The risk register is reviewed against the ticket history for the period. The mobile standard is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is documented alongside the previous year's assessment. The endpoint baseline is evidenced by the quarterly review notes. The remote access path is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The mobile standard is compared with the most recent exercise record. The hardened build is evidenced by the approved design baseline. Each administrative account is traced to the most recent exercise record. The control is tested at least once every twelve months.

The hardened build is validated by the signed exception log. The continuity plan is compared with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Plate 375

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 375 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is measured against the most recent exercise record. The vendor register is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is checked against the approved design baseline. The backup rotation is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is traced to the approved design baseline. The physical controls is traced to the agreed service level. The metric set is evidenced by the register of exceptions. The asset register is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is reconciled with the commissioning document. The asset register is reconciled with the dependency map. Every internet-facing service is documented alongside the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The threat model is traced to the commissioning document. The cloud baseline is measured against the register of exceptions. The retention schedule is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

Plate 376

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 376 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is reviewed against the evidence pack held by the owner. The vendor register is traced to the previous year's assessment. The awareness cycle is compared with the signed exception log. Any deviation requires written approval and an expiry date.

The threat model is reconciled with the signed exception log. The encryption standard is evidenced by the dependency map. The endpoint baseline is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The physical controls is traced to the dependency map. The awareness cycle is validated by the signed exception log. The asset register is evidenced by the commissioning document. The retention schedule is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The physical controls is measured against the register of exceptions. Each administrative account is compared with the current written standard. The vendor register is documented alongside the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is evidenced by the dependency map. The segmentation boundary is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

Plate 377

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 377 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is reconciled with the quarterly review notes. Each administrative account is validated by the approved design baseline. The access review process is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is checked against the previous year's assessment. The monitoring pipeline is traced to the ticket history for the period. Records are retained only as long as the schedule requires.

The metric set is evidenced by the previous year's assessment. The vendor register is compared with the dependency map. The classification scheme is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is validated by the signed exception log. The awareness cycle is traced to the previous year's assessment. The access review process is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

Every internet-facing service is traced to the quarterly review notes. The change process is compared with the quarterly review notes. The encryption standard is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 378

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 378 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is measured against the approved design baseline. The asset register is documented alongside the register of exceptions. The access review process is evidenced by the ticket history for the period. The physical controls is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The asset register is documented alongside the commissioning document. Every internet-facing service is documented alongside the current written standard. The classification scheme is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the ticket history for the period. The physical controls is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the evidence pack held by the owner. Each administrative account is validated by the current written standard. The third-party register is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

Plate 379

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 379 - 232 x 232 px, DeviceRGB, FlateDecode

- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.

- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Test result attached to the record.
- Evidence stored in the shared evidence pack.

The continuity plan is evidenced by the previous year's assessment. The awareness cycle is reconciled with the current written standard. The identity lifecycle is reviewed against the approved design baseline. The email authentication record is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

Plate 380

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 380 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is traced to the register of exceptions. The continuity plan is evidenced by the most recent exercise record. Each administrative account is evidenced by the commissioning document. Each administrative account is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

The mobile standard is evidenced by the register of exceptions. The identity lifecycle is validated by the agreed service level. Any deviation requires written approval and an expiry date.

The continuity plan is checked against the approved design baseline. The access review process is traced to the evidence pack held by the owner. The change process is compared with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is checked against the current written standard. The vulnerability queue is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

Plate 381

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 381 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reconciled with the dependency map. The vulnerability queue is compared with the agreed service level. Metrics are reported as trends rather than single data points.

The physical controls is validated by the ticket history for the period. The physical controls is evidenced by the approved design baseline. The metric set is checked against the commissioning document. The control is tested at least once every twelve months.

Every internet-facing service is evidenced by the current written standard. The identity lifecycle is checked against the most recent exercise record. Each administrative account is documented alongside the dependency map. The risk register is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

Plate 382

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 382 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is checked against the evidence pack held by the owner. The mobile standard is validated by the approved design baseline. The monitoring pipeline is documented alongside the current written standard. The recovery test is validated by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is validated by the previous year's assessment. The continuity plan is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The encryption standard is checked against the ticket history for the period. The backup rotation is evidenced by the agreed service level. The hardened build is traced to the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is compared with the previous year's assessment. The segmentation boundary is evidenced by the most recent exercise record. The hardened build is checked against the register of exceptions. The awareness cycle is traced to the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Plate 383

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 383 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is documented alongside the most recent exercise record. The endpoint baseline is measured against the dependency map. The metric set is validated by the most recent exercise record. Each administrative account is checked against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is validated by the ticket history for the period. The endpoint baseline is validated by the current written standard. The backup rotation is reviewed against the agreed service level. The access review process is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is measured against the ticket history for the period. The backup rotation is traced to the ticket history for the period. The patch calendar is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The retention schedule is traced to the previous year's assessment. The threat model is checked against the evidence pack held by the owner. The change process is traced to the previous year's assessment. The control is tested at least once every twelve months.

Plate 384

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 384 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is reviewed against the most recent exercise record. The vulnerability queue is compared with the approved design baseline. The metric set is documented alongside the signed exception log. The mobile standard is validated by the current written standard. Third parties must demonstrate the control before access is granted.

The segmentation boundary is evidenced by the commissioning document. The risk register is evidenced by the approved design baseline. Every internet-facing service is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

The privileged access list is documented alongside the register of exceptions. The retention schedule is evidenced by the commissioning document. The backup rotation is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is traced to the quarterly review notes. The remote access path is documented alongside the ticket history for the period. Third parties must demonstrate the control before access is granted.

The recovery test is measured against the most recent exercise record. The physical controls is compared with the agreed service level. The email authentication record is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

Plate 385

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 385 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is measured against the previous year's assessment. The risk register is compared with the commissioning document. The hardened build is checked against the quarterly review notes. The control is tested at least once every twelve months.

The privileged access list is reconciled with the previous year's assessment. The mobile standard is compared with the commissioning document. Each administrative account is reviewed against the quarterly review notes. The continuity plan is compared with the current written standard. Third parties must demonstrate the control before access is granted.

The classification scheme is reviewed against the approved design baseline. Each administrative account is evidenced by the dependency map. The vendor register is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Review date scheduled and visible.

Plate 386

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 386 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is reviewed against the ticket history for the period. The mobile standard is validated by the commissioning document. The monitoring pipeline is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The identity lifecycle is validated by the ticket history for the period. The vulnerability queue is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The retention schedule is documented alongside the approved design baseline. The backup rotation is documented alongside the dependency map. Each administrative account is reviewed against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Plate 387

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 387 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is compared with the current written standard. The metric set is reviewed against the evidence pack held by the owner. The privileged access list is traced to the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is reviewed against the most recent exercise record. The retention schedule is measured against the approved design baseline. The continuity plan is compared with the most recent exercise record. The classification scheme is traced to the register of exceptions. Records are retained only as long as the schedule requires.

The endpoint baseline is reconciled with the commissioning document. Each administrative account is compared with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is validated by the most recent exercise record. The backup rotation is traced to the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is reviewed against the previous year's assessment. The encryption standard is evidenced by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Plate 388

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 388 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is compared with the quarterly review notes. The access review process is evidenced by the current written standard. The remote access path is compared with the dependency map. The physical controls is checked against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The privileged access list is reviewed against the approved design baseline. The backup rotation is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

The patch calendar is validated by the quarterly review notes. The retention schedule is evidenced by the previous year's assessment. The monitoring pipeline is reconciled with the signed exception log. The mobile standard is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

The third-party register is documented alongside the current written standard. Every internet-facing service is checked against the register of exceptions. The vendor register is compared with the current written standard. The remote access path is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Plate 389

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 389 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is traced to the register of exceptions. The mobile standard is traced to the agreed service level. The threat model is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The physical controls is reviewed against the agreed service level. The access review process is traced to the quarterly review notes. The asset register is reviewed against the most recent exercise record. The physical controls is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The risk register is traced to the approved design baseline. The endpoint baseline is validated by the register of exceptions. The patch calendar is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is compared with the approved design baseline. The monitoring pipeline is traced to the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The retention schedule is validated by the approved design baseline. The endpoint baseline is checked against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Plate 390

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 390 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is checked against the commissioning document. The risk register is reviewed against the register of exceptions. The physical controls is evidenced by the commissioning document. Third parties must demonstrate the control before access is granted.

The remote access path is measured against the approved design baseline. The patch calendar is reconciled with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is documented alongside the commissioning document. The asset register is compared with the ticket history for the period. The vulnerability queue is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is validated by the current written standard. The vulnerability queue is evidenced by the quarterly review notes. The physical controls is measured against the dependency map. Third parties must demonstrate the control before access is granted.

100. The vulnerability queue

Plate 391

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 391 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is traced to the current written standard. The classification scheme is documented alongside the signed exception log. Any deviation requires written approval and an expiry date.

The vulnerability queue is validated by the most recent exercise record. The monitoring pipeline is checked against the dependency map. The vulnerability queue is compared with the register of exceptions. The control is tested at least once every twelve months.

The monitoring pipeline is reviewed against the signed exception log. The email authentication record is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

The asset register is validated by the ticket history for the period. Each administrative account is validated by the current written standard. The privileged access list is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is reconciled with the agreed service level. Every internet-facing service is traced to the register of exceptions. Any deviation requires written approval and an expiry date.

Plate 392

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 392 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is reviewed against the agreed service level. The cloud baseline is validated by the most recent exercise record. Metrics are reported as trends rather than single data points.

The third-party register is documented alongside the agreed service level. The change process is documented alongside the agreed service level. The patch calendar is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is compared with the dependency map. The segmentation boundary is reviewed against the commissioning document. The risk register is validated by the ticket history for the period. The risk register is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The patch calendar is traced to the ticket history for the period. The privileged access list is validated by the ticket history for the period. The metric set is reviewed against the most recent exercise record. The encryption standard is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Plate 393

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 393 - 232 x 232 px, DeviceRGB, FlateDecode

- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The mobile standard is evidenced by the evidence pack held by the owner. The email authentication record is checked against the agreed service level. The classification scheme is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is validated by the commissioning document. The backup rotation is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is checked against the approved design baseline. The awareness cycle is checked against the quarterly review notes. Any deviation requires written approval and an expiry date.

Plate 394

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 394 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is documented alongside the previous year's assessment. The recovery test is traced to the evidence pack held by the owner. The endpoint baseline is measured against the current written standard. The access review process is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The cloud baseline is reviewed against the ticket history for the period. The mobile standard is traced to the register of exceptions. The classification scheme is traced to the dependency map. The email authentication record is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

The retention schedule is reviewed against the register of exceptions. The risk register is measured against the agreed service level. The endpoint baseline is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is measured against the evidence pack held by the owner. The email authentication record is traced to the quarterly review notes. Each administrative account is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 395

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 395 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is checked against the evidence pack held by the owner. The retention schedule is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is reconciled with the dependency map. The retention schedule is compared with the register of exceptions. The encryption standard is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

Every internet-facing service is reviewed against the signed exception log. The remote access path is reconciled with the agreed service level. The privileged access list is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is compared with the previous year's assessment. The metric set is validated by the signed exception log. The asset register is validated by the current written standard. Every internet-facing service is validated by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The metric set is documented alongside the evidence pack held by the owner. The metric set is traced to the commissioning document. The access review process is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Plate 396

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 396 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is checked against the previous year's assessment. The asset register is reconciled with the signed exception log. The control is tested at least once every twelve months.

Each administrative account is reviewed against the approved design baseline. The cloud baseline is traced to the evidence pack held by the owner. Each administrative account is traced to the current written standard. Metrics are reported as trends rather than single data points.

The cloud baseline is checked against the ticket history for the period. The backup rotation is reconciled with the register of exceptions. The monitoring pipeline is validated by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is compared with the most recent exercise record. The asset register is evidenced by the evidence pack held by the owner. The awareness cycle is validated by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The access review process is reviewed against the previous year's assessment. The third-party register is documented alongside the dependency map. The identity lifecycle is validated by the quarterly review notes. Each administrative account is checked against the quarterly review notes. Any deviation requires written approval and an expiry date.

Plate 397

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 397 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is checked against the agreed service level. The change process is compared with the current written standard. The classification scheme is compared with the signed exception log. The threat model is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is evidenced by the evidence pack held by the owner. The patch calendar is validated by the most recent exercise record. The continuity plan is reconciled with the previous year's assessment. The continuity plan is documented alongside the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The retention schedule is evidenced by the signed exception log. The backup rotation is evidenced by the commissioning document. Records are retained only as long as the schedule requires.

102. The identity lifecycle

The backup rotation is documented alongside the signed exception log. The cloud baseline is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

Plate 398

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 398 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is documented alongside the current written standard. The identity lifecycle is reviewed against the evidence pack held by the owner. The remote access path is checked against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is evidenced by the most recent exercise record. The vendor register is validated by the approved design baseline. The access review process is reconciled with the current written standard. Evidence is kept for audit, insurance and regulator requests.

The recovery test is traced to the most recent exercise record. The risk register is checked against the dependency map. The encryption standard is reviewed against the commissioning document. Each administrative account is compared with the register of exceptions. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the dependency map. The vulnerability queue is validated by the ticket history for the period. The change process is checked against the most recent exercise record. The hardened build is checked against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Plate 399

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 399 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is measured against the approved design baseline. The identity lifecycle is checked against the signed exception log. The intent is to make the safe path the default rather than an exception.

The retention schedule is traced to the evidence pack held by the owner. The risk register is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The risk register is documented alongside the ticket history for the period. The metric set is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The patch calendar is checked against the signed exception log. The cloud baseline is checked against the commissioning document. The threat model is reviewed against the approved design baseline. Records are retained only as long as the schedule requires.

The cloud baseline is evidenced by the commissioning document. The hardened build is checked against the signed exception log. The segmentation boundary is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 400

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 400 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is reconciled with the commissioning document. The privileged access list is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The risk register is measured against the quarterly review notes. The continuity plan is evidenced by the commissioning document. The endpoint baseline is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is validated by the commissioning document. The patch calendar is reviewed against the quarterly review notes. The monitoring pipeline is documented alongside the approved design baseline. The backup rotation is measured against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

103. The awareness cycle

The continuity plan is validated by the quarterly review notes. The asset register is reconciled with the quarterly review notes. The asset register is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 401

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 401 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is validated by the commissioning document. The access review process is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The endpoint baseline is compared with the previous year's assessment. The backup rotation is reconciled with the most recent exercise record. The cloud baseline is reviewed against the signed exception log. Every internet-facing service is validated by the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

104. The retention schedule

Plate 402

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 402 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is validated by the approved design baseline. The threat model is compared with the dependency map. Metrics are reported as trends rather than single data points.

The third-party register is compared with the previous year's assessment. The cloud baseline is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

The mobile standard is reconciled with the evidence pack held by the owner. The remote access path is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is compared with the ticket history for the period. The physical controls is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.

Plate 403

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 403 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is reviewed against the evidence pack held by the owner. The vulnerability queue is evidenced by the previous year's assessment. The recovery test is validated by the dependency map. The monitoring pipeline is evidenced by the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is documented alongside the most recent exercise record. The cloud baseline is validated by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is measured against the agreed service level. The patch calendar is checked against the register of exceptions. The physical controls is traced to the commissioning document. The change process is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The recovery test is reconciled with the register of exceptions. The hardened build is compared with the current written standard. Testing covers the failure case, not only the happy path.

The third-party register is evidenced by the quarterly review notes. The cloud baseline is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Plate 404

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 404 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is documented alongside the current written standard. The asset register is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is checked against the ticket history for the period. The remote access path is measured against the commissioning document. The access review process is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The continuity plan is reconciled with the commissioning document. The retention schedule is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The vendor register is checked against the most recent exercise record. The encryption standard is reconciled with the agreed service level. The encryption standard is compared with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vendor register is documented alongside the register of exceptions. The metric set is evidenced by the evidence pack held by the owner. The email authentication record is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Plate 405

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 405 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reviewed against the ticket history for the period. The change process is measured against the most recent exercise record. Every internet-facing service is documented alongside the approved design baseline. The cloud baseline is checked against the ticket history for the period. The control is tested at least once every twelve months.

The encryption standard is measured against the previous year's assessment. The hardened build is measured against the signed exception log. The remote access path is compared with the commissioning document. The access review process is reconciled with the dependency map. Metrics are reported as trends rather than single data points.

The classification scheme is documented alongside the previous year's assessment. The identity lifecycle is reconciled with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is checked against the approved design baseline. The encryption standard is validated by the signed exception log. The hardened build is traced to the dependency map. Any deviation requires written approval and an expiry date.

Plate 406

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 406 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is documented alongside the quarterly review notes. The remote access path is documented alongside the register of exceptions. Every internet-facing service is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is documented alongside the commissioning document. The physical controls is checked against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is evidenced by the dependency map. The privileged access list is compared with the register of exceptions. The access review process is reviewed against the signed exception log. The cloud baseline is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

105. The segmentation boundary

The physical controls is validated by the commissioning document. The hardened build is checked against the quarterly review notes. The mobile standard is compared with the quarterly review notes. The patch calendar is checked against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

Plate 407

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 407 - 232 x 232 px, DeviceRGB, FlateDecode

- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.

The access review process is compared with the dependency map. The continuity plan is measured against the approved design baseline. The change process is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The awareness cycle is checked against the ticket history for the period. The retention schedule is checked against the agreed service level. The continuity plan is documented alongside the previous year's assessment. The metric set is evidenced by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Plate 408

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 408 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is reviewed against the most recent exercise record. Each administrative account is traced to the register of exceptions. Metrics are reported as trends rather than single data points.

The monitoring pipeline is measured against the previous year's assessment. The mobile standard is reviewed against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is reviewed against the evidence pack held by the owner. The change process is reviewed against the commissioning document. Any deviation requires written approval and an expiry date.

The retention schedule is documented alongside the evidence pack held by the owner. The mobile standard is compared with the quarterly review notes. The identity lifecycle is traced to the ticket history for the period. The hardened build is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

Plate 409

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 409 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is reviewed against the commissioning document. The vendor register is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is validated by the register of exceptions. The mobile standard is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The vendor register is evidenced by the most recent exercise record. Every internet-facing service is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is traced to the previous year's assessment. The retention schedule is documented alongside the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.

Plate 410

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 410 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is documented alongside the previous year's assessment. The access review process is reconciled with the current written standard. The mobile standard is checked against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is validated by the register of exceptions. The hardened build is reconciled with the agreed service level. The physical controls is validated by the ticket history for the period. The patch calendar is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The access review process is traced to the signed exception log. The awareness cycle is documented alongside the dependency map. The risk register is reviewed against the previous year's assessment. The email authentication record is traced to the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The physical controls is traced to the quarterly review notes. The classification scheme is reconciled with the dependency map. The backup rotation is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

Plate 411

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 411 - 232 x 232 px, DeviceRGB, FlateDecode

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

106. The risk register

The vulnerability queue is checked against the signed exception log. The encryption standard is documented alongside the dependency map. The physical controls is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The patch calendar is reconciled with the commissioning document. The mobile standard is reconciled with the previous year's assessment. The awareness cycle is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

- Test result attached to the record.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

Plate 412

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 412 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is documented alongside the evidence pack held by the owner. The backup rotation is measured against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is compared with the previous year's assessment. The change process is evidenced by the signed exception log. The email authentication record is validated by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is traced to the register of exceptions. The cloud baseline is reviewed against the agreed service level. The third-party register is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The metric set is compared with the previous year's assessment. The monitoring pipeline is validated by the register of exceptions. The backup rotation is documented alongside the register of exceptions. The endpoint baseline is traced to the register of exceptions. The control is tested at least once every twelve months.

Plate 413

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 413 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reviewed against the signed exception log. The awareness cycle is traced to the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is documented alongside the agreed service level. Every internet-facing service is documented alongside the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The hardened build is validated by the dependency map. The patch calendar is measured against the commissioning document. The segmentation boundary is reviewed against the most recent exercise record. The backup rotation is reconciled with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is reconciled with the dependency map. The retention schedule is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is documented alongside the commissioning document. The identity lifecycle is compared with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Plate 414

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 414 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is validated by the dependency map. The recovery test is validated by the most recent exercise record. The recovery test is evidenced by the most recent exercise record. The recovery test is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

The awareness cycle is compared with the signed exception log. The mobile standard is measured against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The third-party register is traced to the evidence pack held by the owner. The vulnerability queue is traced to the ticket history for the period. The risk register is measured against the approved design baseline. The mobile standard is compared with the current written standard. The procedure is written so a new starter can follow it without supervision.

107. The continuity plan

The segmentation boundary is validated by the current written standard. The vendor register is compared with the commissioning document. The change process is traced to the register of exceptions. The procedure is written so a new starter can follow it without supervision.

Plate 415

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 415 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is evidenced by the register of exceptions. The access review process is compared with the previous year's assessment. Records are retained only as long as the schedule requires.

108. The remote access path

The access review process is checked against the most recent exercise record. The third-party register is reviewed against the register of exceptions. The access review process is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is validated by the current written standard. The risk register is validated by the signed exception log. The control is tested at least once every twelve months.

The encryption standard is checked against the quarterly review notes. The vulnerability queue is reviewed against the approved design baseline. The threat model is reviewed against the approved design baseline. Every internet-facing service is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Plate 416

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 416 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is compared with the approved design baseline. The asset register is compared with the previous year's assessment. The asset register is documented alongside the signed exception log. The identity lifecycle is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The change process is reconciled with the evidence pack held by the owner. The asset register is reviewed against the signed exception log. The patch calendar is documented alongside the signed exception log. The retention schedule is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

109. The identity lifecycle

The physical controls is reconciled with the agreed service level. The recovery test is validated by the register of exceptions. The backup rotation is compared with the signed exception log. The continuity plan is reviewed against the agreed service level. The control is tested at least once every twelve months.

Plate 417

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 417 - 232 x 232 px, DeviceRGB, FlateDecode

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.

The risk register is documented alongside the signed exception log. The asset register is evidenced by the approved design baseline. The vulnerability queue is compared with the agreed service level. The monitoring pipeline is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Test result attached to the record.

The email authentication record is reconciled with the quarterly review notes. The encryption standard is evidenced by the most recent exercise record. The cloud baseline is evidenced by the signed exception log. The vulnerability queue is evidenced by the dependency map. Testing covers the failure case, not only the happy path.

Plate 418

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 418 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is validated by the evidence pack held by the owner. The continuity plan is reconciled with the evidence pack held by the owner. The remote access path is validated by the evidence pack held by the owner. The identity lifecycle is documented alongside the current written standard. The intent is to make the safe path the default rather than an exception.

The metric set is reviewed against the ticket history for the period. Each administrative account is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is evidenced by the register of exceptions. The hardened build is reviewed against the evidence pack held by the owner. The identity lifecycle is measured against the commissioning document. The segmentation boundary is documented alongside the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The change process is evidenced by the dependency map. The privileged access list is measured against the agreed service level. Testing covers the failure case, not only the happy path.

Plate 419

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 419 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is evidenced by the agreed service level. The third-party register is documented alongside the most recent exercise record. The classification scheme is measured against the dependency map. The awareness cycle is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

The physical controls is measured against the approved design baseline. The vendor register is checked against the previous year's assessment. The encryption standard is evidenced by the evidence pack held by the owner. The identity lifecycle is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The continuity plan is reviewed against the quarterly review notes. The backup rotation is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The change process is reconciled with the current written standard. The continuity plan is validated by the evidence pack held by the owner. The awareness cycle is evidenced by the register of exceptions. Third parties must demonstrate the control before access is granted.

Plate 420

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 420 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reviewed against the register of exceptions. The physical controls is validated by the approved design baseline. The backup rotation is validated by the quarterly review notes. The control is tested at least once every twelve months.

The vendor register is measured against the register of exceptions. The retention schedule is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is documented alongside the approved design baseline. The endpoint baseline is traced to the evidence pack held by the owner. The threat model is evidenced by the current written standard. Evidence is kept for audit, insurance and regulator requests.

- Exception route documented and time-bound.
- Test result attached to the record.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

Plate 421

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 421 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is evidenced by the approved design baseline. The continuity plan is evidenced by the current written standard. The threat model is validated by the register of exceptions. The patch calendar is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The retention schedule is reviewed against the commissioning document. The risk register is measured against the approved design baseline. The third-party register is measured against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is validated by the current written standard. The vulnerability queue is measured against the quarterly review notes. The patch calendar is reviewed against the signed exception log. The privileged access list is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is evidenced by the register of exceptions. The asset register is compared with the most recent exercise record. The classification scheme is compared with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 422

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 422 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is checked against the signed exception log. The segmentation boundary is reviewed against the current written standard. The backup rotation is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is reconciled with the register of exceptions. The privileged access list is evidenced by the current written standard. Testing covers the failure case, not only the happy path.

110. The identity lifecycle

The physical controls is traced to the agreed service level. The vulnerability queue is validated by the commissioning document. Each administrative account is validated by the signed exception log. The backup rotation is measured against the register of exceptions. The control is tested at least once every twelve months.

The patch calendar is traced to the signed exception log. The awareness cycle is measured against the agreed service level. The continuity plan is traced to the agreed service level. The monitoring pipeline is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 423

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 423 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reviewed against the evidence pack held by the owner. The asset register is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is validated by the commissioning document. The risk register is checked against the most recent exercise record. The recovery test is checked against the commissioning document. The email authentication record is validated by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The change process is measured against the agreed service level. The metric set is evidenced by the commissioning document. The continuity plan is traced to the dependency map. The vendor register is documented alongside the commissioning document. Third parties must demonstrate the control before access is granted.

The metric set is compared with the agreed service level. The asset register is compared with the quarterly review notes. The encryption standard is checked against the quarterly review notes. The encryption standard is compared with the approved design baseline. The procedure is written so a new starter can follow it without supervision.

Plate 424

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 424 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is reconciled with the dependency map. The physical controls is reconciled with the current written standard. The cloud baseline is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The identity lifecycle is measured against the approved design baseline. The segmentation boundary is compared with the dependency map. The asset register is compared with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is evidenced by the most recent exercise record. The risk register is evidenced by the evidence pack held by the owner. The third-party register is traced to the quarterly review notes. The remote access path is validated by the register of exceptions. The control is tested at least once every twelve months.

The endpoint baseline is measured against the ticket history for the period. The metric set is checked against the most recent exercise record. The physical controls is traced to the dependency map. Testing covers the failure case, not only the happy path.

Plate 425

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 425 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is measured against the ticket history for the period. Every internet-facing service is evidenced by the current written standard. The mobile standard is reviewed against the dependency map. The metric set is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is reconciled with the ticket history for the period. The cloud baseline is reconciled with the commissioning document. The awareness cycle is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The change process is reconciled with the quarterly review notes. The awareness cycle is checked against the signed exception log. The risk register is traced to the evidence pack held by the owner. The threat model is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

The physical controls is reconciled with the signed exception log. The remote access path is reviewed against the dependency map. The backup rotation is checked against the register of exceptions. The continuity plan is checked against the current written standard. Records are retained only as long as the schedule requires.

Plate 426

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 426 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is validated by the evidence pack held by the owner. The vendor register is reconciled with the quarterly review notes. The vendor register is documented alongside the quarterly review notes. The classification scheme is reviewed against the agreed service level. The control is tested at least once every twelve months.

- Test result attached to the record.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Notification list confirmed before execution.

The mobile standard is documented alongside the ticket history for the period. The cloud baseline is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The recovery test is validated by the dependency map. The awareness cycle is traced to the commissioning document. Any deviation requires written approval and an expiry date.

Plate 427

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 427 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is traced to the evidence pack held by the owner. The mobile standard is reconciled with the commissioning document. The encryption standard is traced to the quarterly review notes. Third parties must demonstrate the control before access is granted.

The awareness cycle is measured against the agreed service level. The cloud baseline is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The privileged access list is validated by the register of exceptions. The privileged access list is validated by the previous year's assessment. The threat model is checked against the previous year's assessment. The threat model is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

111. The awareness cycle

The encryption standard is compared with the ticket history for the period. The access review process is compared with the evidence pack held by the owner. The asset register is traced to the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 428

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 428 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is validated by the dependency map. The metric set is reconciled with the approved design baseline. The asset register is reconciled with the register of exceptions. The monitoring pipeline is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The remote access path is traced to the most recent exercise record. Every internet-facing service is compared with the quarterly review notes. The encryption standard is reconciled with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The threat model is compared with the agreed service level. The risk register is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

The access review process is traced to the quarterly review notes. The vendor register is measured against the ticket history for the period. The email authentication record is traced to the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 429

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 429 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is evidenced by the commissioning document. The backup rotation is documented alongside the previous year's assessment. The segmentation boundary is evidenced by the agreed service level. The control is tested at least once every twelve months.

Every internet-facing service is validated by the agreed service level. The change process is validated by the quarterly review notes. Each administrative account is documented alongside the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The recovery test is checked against the evidence pack held by the owner. The third-party register is traced to the commissioning document. Each administrative account is validated by the evidence pack held by the owner. The cloud baseline is documented alongside the register of exceptions. Metrics are reported as trends rather than single data points.

The monitoring pipeline is validated by the agreed service level. The vulnerability queue is measured against the register of exceptions. The email authentication record is compared with the quarterly review notes. Metrics are reported as trends rather than single data points.

The hardened build is measured against the signed exception log. The recovery test is validated by the current written standard. The cloud baseline is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 430

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 430 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is compared with the dependency map. The third-party register is validated by the previous year's assessment. The remote access path is measured against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The backup rotation is validated by the signed exception log. The awareness cycle is checked against the commissioning document. The access review process is reconciled with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The recovery test is reconciled with the previous year's assessment. The asset register is validated by the dependency map. The mobile standard is reconciled with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is compared with the previous year's assessment. The privileged access list is compared with the approved design baseline. The asset register is reconciled with the current written standard. The segmentation boundary is measured against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is validated by the approved design baseline. The endpoint baseline is evidenced by the most recent exercise record. The hardened build is compared with the dependency map. The control is tested at least once every twelve months.

Plate 431

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 431 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is evidenced by the previous year's assessment. The hardened build is checked against the dependency map. Records are retained only as long as the schedule requires.

The physical controls is documented alongside the ticket history for the period. The backup rotation is documented alongside the register of exceptions. The change process is evidenced by the agreed service level. The vulnerability queue is documented alongside the most recent exercise record. Testing covers the failure case, not only the happy path.

112. The recovery test

The privileged access list is documented alongside the evidence pack held by the owner. The segmentation boundary is reconciled with the agreed service level. The metric set is checked against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is evidenced by the commissioning document. The hardened build is documented alongside the evidence pack held by the owner. The email authentication record is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Plate 432

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 432 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is compared with the quarterly review notes. Each administrative account is documented alongside the approved design baseline. Metrics are reported as trends rather than single data points.

- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.

The awareness cycle is reviewed against the commissioning document. The mobile standard is documented alongside the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is compared with the ticket history for the period. The access review process is compared with the ticket history for the period. The physical controls is reconciled with the most recent exercise record. The change process is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The privileged access list is compared with the previous year's assessment. The continuity plan is compared with the most recent exercise record. The hardened build is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

Plate 433

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 433 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is checked against the commissioning document. The email authentication record is checked against the approved design baseline. The access review process is evidenced by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is checked against the agreed service level. The retention schedule is measured against the signed exception log. The segmentation boundary is evidenced by the agreed service level. Records are retained only as long as the schedule requires.

The segmentation boundary is traced to the register of exceptions. The metric set is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The metric set is documented alongside the previous year's assessment. The identity lifecycle is traced to the most recent exercise record. Every internet-facing service is validated by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

113. The cloud baseline

The vulnerability queue is evidenced by the dependency map. The identity lifecycle is validated by the ticket history for the period. The recovery test is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

Plate 434

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 434 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is reviewed against the quarterly review notes. The asset register is evidenced by the ticket history for the period. The risk register is evidenced by the approved design baseline. The mobile standard is documented alongside the evidence pack held by the owner. The control is tested at least once every twelve months.

The backup rotation is traced to the register of exceptions. The continuity plan is compared with the dependency map. The patch calendar is measured against the dependency map. The retention schedule is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

Plate 435

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 435 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is reconciled with the agreed service level. The classification scheme is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The retention schedule is measured against the previous year's assessment. The email authentication record is traced to the approved design baseline. The third-party register is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is evidenced by the register of exceptions. The vulnerability queue is reconciled with the agreed service level. The remote access path is compared with the register of exceptions. The encryption standard is evidenced by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

Plate 436

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 436 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reconciled with the commissioning document. The vulnerability queue is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

114. The metric set

The physical controls is validated by the most recent exercise record. The patch calendar is reconciled with the quarterly review notes. The recovery test is reconciled with the current written standard. Records are retained only as long as the schedule requires.

The patch calendar is traced to the quarterly review notes. The access review process is validated by the signed exception log. The patch calendar is reconciled with the approved design baseline. The threat model is measured against the dependency map. The control is tested at least once every twelve months.

The asset register is reviewed against the quarterly review notes. The threat model is reviewed against the dependency map. The asset register is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

Plate 437

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 437 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is reconciled with the previous year's assessment. Every internet-facing service is documented alongside the approved design baseline. The patch calendar is reconciled with the current written standard. The third-party register is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The risk register is documented alongside the evidence pack held by the owner. The endpoint baseline is reconciled with the current written standard. The change process is compared with the ticket history for the period. The email authentication record is reconciled with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.

The cloud baseline is reconciled with the dependency map. The awareness cycle is compared with the approved design baseline. The endpoint baseline is checked against the register of exceptions. The encryption standard is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 438

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 438 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is checked against the most recent exercise record. The retention schedule is traced to the current written standard. The email authentication record is reviewed against the signed exception log. The remote access path is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the current written standard. The recovery test is reviewed against the quarterly review notes. The access review process is reconciled with the signed exception log. Every internet-facing service is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Review date scheduled and visible.

Plate 439

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 439 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is evidenced by the approved design baseline. The threat model is documented alongside the previous year's assessment. The physical controls is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is evidenced by the register of exceptions. The identity lifecycle is documented alongside the register of exceptions. Any deviation requires written approval and an expiry date.

The asset register is evidenced by the previous year's assessment. The change process is reviewed against the dependency map. The awareness cycle is checked against the agreed service level. The continuity plan is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The remote access path is validated by the commissioning document. The risk register is documented alongside the evidence pack held by the owner. The vulnerability queue is checked against the current written standard. The monitoring pipeline is evidenced by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is traced to the commissioning document. The physical controls is validated by the approved design baseline. Records are retained only as long as the schedule requires.

Plate 440

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 440 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is checked against the signed exception log. The remote access path is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The vendor register is compared with the approved design baseline. The backup rotation is evidenced by the previous year's assessment. The metric set is checked against the most recent exercise record. The risk register is evidenced by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is checked against the agreed service level. The physical controls is validated by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The recovery test is evidenced by the approved design baseline. The risk register is documented alongside the evidence pack held by the owner. The segmentation boundary is measured against the approved design baseline. Records are retained only as long as the schedule requires.

The backup rotation is reviewed against the quarterly review notes. The recovery test is checked against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

Plate 441

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 441 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is documented alongside the most recent exercise record. The vulnerability queue is evidenced by the most recent exercise record. The threat model is measured against the commissioning document. Testing covers the failure case, not only the happy path.

The patch calendar is checked against the register of exceptions. The vulnerability queue is reconciled with the dependency map. The recovery test is traced to the dependency map. Each administrative account is compared with the quarterly review notes. The control is tested at least once every twelve months.

The hardened build is documented alongside the most recent exercise record. The backup rotation is reviewed against the quarterly review notes. The continuity plan is reconciled with the evidence pack held by the owner. Each administrative account is measured against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is validated by the dependency map. The endpoint baseline is documented alongside the signed exception log. The change process is validated by the signed exception log. Each administrative account is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 442

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 442 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is compared with the ticket history for the period. The third-party register is evidenced by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The recovery test is checked against the most recent exercise record. The email authentication record is compared with the quarterly review notes. The control is tested at least once every twelve months.

The metric set is checked against the dependency map. The third-party register is checked against the current written standard. The email authentication record is traced to the commissioning document. The physical controls is evidenced by the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The threat model is validated by the most recent exercise record. The hardened build is validated by the dependency map. The email authentication record is measured against the most recent exercise record. The remote access path is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Plate 443

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 443 - 232 x 232 px, DeviceRGB, FlateDecode

115. The vendor register

The vulnerability queue is checked against the signed exception log. The retention schedule is traced to the most recent exercise record. The vendor register is reconciled with the dependency map. Records are retained only as long as the schedule requires.

The risk register is validated by the quarterly review notes. The remote access path is evidenced by the agreed service level. The email authentication record is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The physical controls is reconciled with the commissioning document. The physical controls is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.

Plate 444

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 444 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is validated by the current written standard. The change process is compared with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The risk register is compared with the most recent exercise record. The backup rotation is compared with the current written standard. Metrics are reported as trends rather than single data points.

116. The risk register

The identity lifecycle is compared with the agreed service level. The change process is documented alongside the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is measured against the register of exceptions. The vendor register is measured against the register of exceptions. The retention schedule is measured against the signed exception log. The recovery test is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

Plate 445

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 445 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is traced to the evidence pack held by the owner. The classification scheme is reconciled with the ticket history for the period. Each administrative account is validated by the register of exceptions. The remote access path is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is measured against the previous year's assessment. The asset register is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The vendor register is checked against the quarterly review notes. The third-party register is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

The vulnerability queue is reviewed against the ticket history for the period. The encryption standard is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is reviewed against the previous year's assessment. The backup rotation is traced to the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Plate 446

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 446 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is reviewed against the most recent exercise record. Every internet-facing service is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is reviewed against the current written standard. The third-party register is checked against the quarterly review notes. The monitoring pipeline is reviewed against the dependency map. The encryption standard is compared with the register of exceptions. Metrics are reported as trends rather than single data points.

The threat model is reviewed against the ticket history for the period. The change process is checked against the quarterly review notes. The privileged access list is evidenced by the most recent exercise record. The awareness cycle is documented alongside the previous year's assessment. Third parties must demonstrate the control before access is granted.

The change process is reconciled with the previous year's assessment. The backup rotation is compared with the most recent exercise record. The mobile standard is checked against the signed exception log. The endpoint baseline is validated by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 447

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 447 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is checked against the previous year's assessment. The hardened build is documented alongside the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The risk register is reviewed against the evidence pack held by the owner. The privileged access list is measured against the evidence pack held by the owner. The endpoint baseline is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The access review process is compared with the ticket history for the period. The remote access path is evidenced by the most recent exercise record. The third-party register is reconciled with the approved design baseline. The encryption standard is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is traced to the quarterly review notes. The hardened build is validated by the evidence pack held by the owner. Each administrative account is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Plate 448

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 448 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is checked against the evidence pack held by the owner. The retention schedule is checked against the most recent exercise record. The vendor register is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is reconciled with the register of exceptions. Each administrative account is checked against the register of exceptions. The vendor register is traced to the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The retention schedule is documented alongside the approved design baseline. The retention schedule is validated by the dependency map. The vulnerability queue is measured against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The metric set is documented alongside the previous year's assessment. The mobile standard is reviewed against the register of exceptions. The identity lifecycle is compared with the evidence pack held by the owner. The privileged access list is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Plate 449

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 449 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is compared with the current written standard. The hardened build is checked against the evidence pack held by the owner. The metric set is documented alongside the signed exception log. Records are retained only as long as the schedule requires.

The privileged access list is evidenced by the current written standard. The risk register is reconciled with the agreed service level. The asset register is checked against the ticket history for the period. Every internet-facing service is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The third-party register is checked against the previous year's assessment. The remote access path is documented alongside the most recent exercise record. The vulnerability queue is reconciled with the agreed service level. The backup rotation is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The threat model is reconciled with the most recent exercise record. The continuity plan is evidenced by the commissioning document. Each administrative account is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

Plate 450

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 450 - 232 x 232 px, DeviceRGB, FlateDecode

The vendor register is compared with the evidence pack held by the owner. The hardened build is measured against the commissioning document. The intent is to make the safe path the default rather than an exception.

Each administrative account is traced to the evidence pack held by the owner. The risk register is evidenced by the register of exceptions. The mobile standard is documented alongside the quarterly review notes. The control is tested at least once every twelve months.

The endpoint baseline is reconciled with the most recent exercise record. The backup rotation is reconciled with the ticket history for the period. The cloud baseline is documented alongside the commissioning document. The control is tested at least once every twelve months.

The encryption standard is compared with the register of exceptions. The vendor register is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The change process is validated by the current written standard. The cloud baseline is measured against the current written standard. The change process is measured against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

Plate 451

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 451 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is traced to the previous year's assessment. The mobile standard is reviewed against the quarterly review notes. The remote access path is evidenced by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

117. The segmentation boundary

The email authentication record is evidenced by the dependency map. The privileged access list is checked against the previous year's assessment. The vendor register is compared with the commissioning document. The endpoint baseline is compared with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is compared with the dependency map. Each administrative account is traced to the dependency map. The change process is checked against the signed exception log. The vulnerability queue is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

Plate 452

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 452 - 232 x 232 px, DeviceRGB, FlateDecode

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The privileged access list is measured against the signed exception log. The vendor register is reconciled with the quarterly review notes. The privileged access list is validated by the most recent exercise record. The encryption standard is reconciled with the signed exception log. The intent is to make the safe path the default rather than an exception.

118. The threat model

The mobile standard is evidenced by the register of exceptions. Each administrative account is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 453

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 453 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is reviewed against the quarterly review notes. The third-party register is traced to the quarterly review notes. The remote access path is compared with the previous year's assessment. The remote access path is reviewed against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is traced to the agreed service level. The retention schedule is validated by the current written standard. The classification scheme is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The remote access path is reviewed against the agreed service level. The classification scheme is traced to the ticket history for the period. The awareness cycle is validated by the ticket history for the period. The vulnerability queue is validated by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is checked against the quarterly review notes. The mobile standard is checked against the approved design baseline. The privileged access list is checked against the approved design baseline. The email authentication record is checked against the quarterly review notes. The control is tested at least once every twelve months.

Plate 454

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 454 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is evidenced by the ticket history for the period. The recovery test is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is reconciled with the agreed service level. The mobile standard is reviewed against the dependency map. The change process is reviewed against the approved design baseline. The risk register is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

The change process is checked against the evidence pack held by the owner. The change process is reconciled with the signed exception log. The monitoring pipeline is compared with the signed exception log. The identity lifecycle is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is compared with the agreed service level. The asset register is measured against the previous year's assessment. Metrics are reported as trends rather than single data points.

Plate 455

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 455 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is checked against the quarterly review notes. The mobile standard is documented alongside the commissioning document. The continuity plan is measured against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The threat model is evidenced by the agreed service level. The third-party register is reviewed against the quarterly review notes. The endpoint baseline is evidenced by the signed exception log. The hardened build is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is checked against the dependency map. The endpoint baseline is compared with the quarterly review notes. The vendor register is traced to the agreed service level. The access review process is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The metric set is checked against the register of exceptions. The backup rotation is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The remote access path is traced to the register of exceptions. The physical controls is checked against the ticket history for the period. The risk register is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

Plate 456

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 456 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is measured against the previous year's assessment. The vulnerability queue is reconciled with the ticket history for the period. The third-party register is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The threat model is measured against the register of exceptions. The metric set is reviewed against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The vulnerability queue is compared with the register of exceptions. The privileged access list is compared with the agreed service level. The endpoint baseline is reviewed against the most recent exercise record. The cloud baseline is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

The hardened build is documented alongside the evidence pack held by the owner. The awareness cycle is compared with the ticket history for the period. The metric set is measured against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the approved design baseline. The monitoring pipeline is reconciled with the quarterly review notes. The third-party register is validated by the approved design baseline. The vulnerability queue is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

Plate 457

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 457 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is checked against the signed exception log. The third-party register is measured against the register of exceptions. The remote access path is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The access review process is reconciled with the quarterly review notes. The endpoint baseline is checked against the quarterly review notes. The remote access path is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

The cloud baseline is validated by the previous year's assessment. Each administrative account is checked against the most recent exercise record. Every internet-facing service is reviewed against the approved design baseline. The segmentation boundary is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is checked against the agreed service level. The email authentication record is traced to the current written standard. The threat model is checked against the most recent exercise record. Every internet-facing service is traced to the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

Plate 458

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 458 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is evidenced by the commissioning document. The change process is documented alongside the quarterly review notes. The vendor register is compared with the agreed service level. The threat model is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is checked against the signed exception log. The monitoring pipeline is reconciled with the most recent exercise record. The access review process is compared with the current written standard. Any deviation requires written approval and an expiry date.

119. The patch calendar

The privileged access list is compared with the register of exceptions. The third-party register is traced to the current written standard. The physical controls is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is evidenced by the signed exception log. The change process is checked against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Plate 459

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 459 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is checked against the register of exceptions. Each administrative account is traced to the register of exceptions. Any deviation requires written approval and an expiry date.

The endpoint baseline is reviewed against the quarterly review notes. The metric set is checked against the previous year's assessment. The control is tested at least once every twelve months.

The email authentication record is measured against the evidence pack held by the owner. The change process is documented alongside the signed exception log. Metrics are reported as trends rather than single data points.

The risk register is evidenced by the approved design baseline. The remote access path is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The vendor register is documented alongside the register of exceptions. The vendor register is measured against the agreed service level. The risk register is traced to the commissioning document. The intent is to make the safe path the default rather than an exception.

The third-party register is evidenced by the evidence pack held by the owner. The cloud baseline is measured against the current written standard. Records are retained only as long as the schedule requires.

Plate 460

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 460 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is reconciled with the register of exceptions. The mobile standard is compared with the commissioning document. The cloud baseline is reconciled with the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The privileged access list is validated by the commissioning document. The risk register is reconciled with the dependency map. The segmentation boundary is reconciled with the current written standard. The backup rotation is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.

The patch calendar is reviewed against the agreed service level. The asset register is traced to the most recent exercise record. The encryption standard is evidenced by the evidence pack held by the owner. The vendor register is documented alongside the current written standard. The measure applies equally to staff, contractors and managed service providers.

Plate 461

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 461 - 232 x 232 px, DeviceRGB, FlateDecode

120. Every internet-facing service

The encryption standard is measured against the ticket history for the period. The hardened build is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The hardened build is measured against the dependency map. The patch calendar is documented alongside the approved design baseline. The asset register is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is checked against the most recent exercise record. The metric set is validated by the commissioning document. The third-party register is validated by the commissioning document. The monitoring pipeline is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.

The change process is measured against the agreed service level. The access review process is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

Plate 462

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 462 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is reconciled with the previous year's assessment. The email authentication record is checked against the dependency map. Third parties must demonstrate the control before access is granted.

The awareness cycle is compared with the agreed service level. The physical controls is reconciled with the previous year's assessment. The asset register is reconciled with the approved design baseline. The encryption standard is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

121. The retention schedule

The recovery test is validated by the register of exceptions. The vendor register is traced to the ticket history for the period. The email authentication record is documented alongside the current written standard. The remote access path is measured against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is reviewed against the signed exception log. The encryption standard is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

Plate 463

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 463 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is traced to the approved design baseline. The privileged access list is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

The metric set is checked against the commissioning document. The risk register is compared with the ticket history for the period. The vendor register is validated by the current written standard. The hardened build is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vendor register is compared with the evidence pack held by the owner. The vulnerability queue is traced to the commissioning document. The patch calendar is documented alongside the dependency map. Every internet-facing service is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

The segmentation boundary is compared with the signed exception log. Every internet-facing service is validated by the approved design baseline. Metrics are reported as trends rather than single data points.

The identity lifecycle is traced to the signed exception log. The remote access path is traced to the dependency map. The identity lifecycle is reconciled with the dependency map. The backup rotation is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Plate 464

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 464 - 232 x 232 px, DeviceRGB, FlateDecode

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Review date scheduled and visible.
- Notification list confirmed before execution.

Every internet-facing service is documented alongside the signed exception log. The recovery test is validated by the approved design baseline. The email authentication record is traced to the signed exception log. The mobile standard is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is checked against the dependency map. The awareness cycle is reviewed against the dependency map. Evidence is kept for audit, insurance and regulator requests.

Plate 465

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 465 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is documented alongside the register of exceptions. The cloud baseline is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The remote access path is traced to the signed exception log. The cloud baseline is reviewed against the signed exception log. Each administrative account is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The privileged access list is measured against the dependency map. The cloud baseline is checked against the register of exceptions. The email authentication record is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is evidenced by the dependency map. The change process is checked against the commissioning document. Any deviation requires written approval and an expiry date.

The email authentication record is documented alongside the approved design baseline. The metric set is compared with the register of exceptions. The retention schedule is reviewed against the dependency map. The control is tested at least once every twelve months.

Plate 466

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 466 - 232 x 232 px, DeviceRGB, FlateDecode

The email authentication record is traced to the register of exceptions. The threat model is measured against the ticket history for the period. The physical controls is compared with the previous year's assessment. Records are retained only as long as the schedule requires.

Every internet-facing service is measured against the register of exceptions. The recovery test is checked against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is documented alongside the signed exception log. The threat model is compared with the dependency map. The intent is to make the safe path the default rather than an exception.

The awareness cycle is checked against the ticket history for the period. The monitoring pipeline is evidenced by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is compared with the signed exception log. The encryption standard is evidenced by the previous year's assessment. The email authentication record is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

Plate 467

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 467 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is traced to the current written standard. The patch calendar is validated by the register of exceptions. The physical controls is compared with the agreed service level. The privileged access list is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The awareness cycle is measured against the commissioning document. The change process is reviewed against the register of exceptions. The privileged access list is measured against the current written standard. The third-party register is checked against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The hardened build is documented alongside the current written standard. The risk register is reviewed against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The access review process is traced to the most recent exercise record. The endpoint baseline is reviewed against the ticket history for the period. The identity lifecycle is reviewed against the register of exceptions. Each administrative account is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Plate 468

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 468 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is evidenced by the register of exceptions. The cloud baseline is compared with the most recent exercise record. The email authentication record is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is traced to the commissioning document. The access review process is traced to the previous year's assessment. The monitoring pipeline is compared with the most recent exercise record. Metrics are reported as trends rather than single data points.

The vulnerability queue is reconciled with the register of exceptions. The continuity plan is measured against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The risk register is validated by the commissioning document. The privileged access list is validated by the quarterly review notes. The encryption standard is evidenced by the signed exception log. The threat model is validated by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is compared with the ticket history for the period. The threat model is measured against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Plate 469

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 469 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is checked against the ticket history for the period. The retention schedule is reviewed against the agreed service level. The awareness cycle is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is checked against the previous year's assessment. The risk register is measured against the dependency map. The vendor register is checked against the register of exceptions. The remote access path is validated by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The cloud baseline is traced to the agreed service level. The change process is checked against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is compared with the dependency map. The access review process is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The change process is compared with the previous year's assessment. The awareness cycle is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Plate 470

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 470 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is reviewed against the commissioning document. The cloud baseline is documented alongside the approved design baseline. The change process is measured against the most recent exercise record. The segmentation boundary is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The metric set is documented alongside the dependency map. The email authentication record is traced to the signed exception log. Any deviation requires written approval and an expiry date.

The identity lifecycle is traced to the ticket history for the period. The retention schedule is documented alongside the approved design baseline. The vulnerability queue is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The privileged access list is reconciled with the ticket history for the period. The asset register is compared with the most recent exercise record. The segmentation boundary is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is traced to the signed exception log. The privileged access list is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Plate 471

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 471 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is evidenced by the register of exceptions. The vulnerability queue is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is traced to the signed exception log. The classification scheme is measured against the approved design baseline. The physical controls is validated by the most recent exercise record. The access review process is traced to the dependency map. Records are retained only as long as the schedule requires.

The metric set is evidenced by the register of exceptions. Every internet-facing service is documented alongside the commissioning document. The backup rotation is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The endpoint baseline is measured against the approved design baseline. The backup rotation is evidenced by the most recent exercise record. The endpoint baseline is compared with the signed exception log. Testing covers the failure case, not only the happy path.

The backup rotation is evidenced by the most recent exercise record. The classification scheme is reviewed against the agreed service level. Records are retained only as long as the schedule requires.

Plate 472

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 472 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is compared with the dependency map. The threat model is reviewed against the quarterly review notes. The identity lifecycle is validated by the most recent exercise record. The physical controls is evidenced by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The risk register is validated by the register of exceptions. The encryption standard is documented alongside the quarterly review notes. The access review process is measured against the dependency map. The vulnerability queue is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The asset register is measured against the previous year's assessment. The monitoring pipeline is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is reconciled with the dependency map. The metric set is validated by the previous year's assessment. The risk register is validated by the dependency map. The identity lifecycle is reviewed against the most recent exercise record. Any deviation requires written approval and an expiry date.

Plate 473

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 473 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is compared with the current written standard. The patch calendar is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The change process is validated by the current written standard. The awareness cycle is measured against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is documented alongside the agreed service level. The email authentication record is measured against the current written standard. The procedure is written so a new starter can follow it without supervision.

The retention schedule is reviewed against the ticket history for the period. The encryption standard is reconciled with the quarterly review notes. The third-party register is measured against the ticket history for the period. The access review process is reviewed against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is compared with the dependency map. The classification scheme is documented alongside the register of exceptions. The encryption standard is documented alongside the most recent exercise record. The continuity plan is validated by the commissioning document. The control is tested at least once every twelve months.

Plate 474

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 474 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is compared with the quarterly review notes. The segmentation boundary is reviewed against the agreed service level. The privileged access list is evidenced by the most recent exercise record. The vulnerability queue is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

- Exception route documented and time-bound.
- Test result attached to the record.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The identity lifecycle is traced to the approved design baseline. The endpoint baseline is evidenced by the approved design baseline. The access review process is checked against the approved design baseline. The monitoring pipeline is traced to the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is compared with the current written standard. The vendor register is measured against the register of exceptions. The physical controls is reconciled with the commissioning document. The physical controls is traced to the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Plate 475

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 475 - 232 x 232 px, DeviceRGB, FlateDecode

The monitoring pipeline is traced to the agreed service level. The metric set is documented alongside the agreed service level. The change process is checked against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is measured against the quarterly review notes. Every internet-facing service is checked against the most recent exercise record. The encryption standard is evidenced by the register of exceptions. The monitoring pipeline is validated by the quarterly review notes. Records are retained only as long as the schedule requires.

Every internet-facing service is measured against the quarterly review notes. The asset register is reconciled with the signed exception log. The monitoring pipeline is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The access review process is reconciled with the approved design baseline. The physical controls is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

Plate 476

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 476 - 232 x 232 px, DeviceRGB, FlateDecode

The awareness cycle is documented alongside the current written standard. The vendor register is checked against the most recent exercise record. Each administrative account is reviewed against the agreed service level. The physical controls is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is measured against the most recent exercise record. The physical controls is reviewed against the current written standard. The remote access path is documented alongside the ticket history for the period. The classification scheme is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The access review process is validated by the evidence pack held by the owner. The awareness cycle is evidenced by the ticket history for the period. The change process is compared with the approved design baseline. The mobile standard is measured against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is reviewed against the dependency map. The endpoint baseline is traced to the agreed service level. The encryption standard is reconciled with the current written standard. The recovery test is checked against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Plate 477

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 477 - 232 x 232 px, DeviceRGB, FlateDecode

123. The classification scheme

The identity lifecycle is reconciled with the register of exceptions. The recovery test is evidenced by the previous year's assessment. The patch calendar is reconciled with the approved design baseline. The continuity plan is traced to the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is compared with the register of exceptions. The retention schedule is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is measured against the signed exception log. The vendor register is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is validated by the evidence pack held by the owner. The risk register is evidenced by the evidence pack held by the owner. The mobile standard is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

Plate 478

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 478 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is traced to the current written standard. The backup rotation is evidenced by the current written standard. The asset register is checked against the previous year's assessment. Any deviation requires written approval and an expiry date.

The awareness cycle is reviewed against the current written standard. The third-party register is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is documented alongside the current written standard. The classification scheme is checked against the signed exception log. The risk register is measured against the dependency map. Metrics are reported as trends rather than single data points.

The physical controls is reviewed against the dependency map. The access review process is traced to the agreed service level. The physical controls is checked against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is evidenced by the register of exceptions. The patch calendar is validated by the current written standard. The identity lifecycle is documented alongside the agreed service level. The cloud baseline is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

Plate 479

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 479 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is reconciled with the agreed service level. The segmentation boundary is reconciled with the evidence pack held by the owner. The third-party register is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is documented alongside the most recent exercise record. The identity lifecycle is validated by the signed exception log. The vendor register is reconciled with the commissioning document. The awareness cycle is compared with the commissioning document. The intent is to make the safe path the default rather than an exception.

The cloud baseline is measured against the current written standard. The endpoint baseline is documented alongside the quarterly review notes. The control is tested at least once every twelve months.

The recovery test is compared with the approved design baseline. The threat model is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is documented alongside the quarterly review notes. The retention schedule is validated by the signed exception log. The backup rotation is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

Plate 480

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 480 - 232 x 232 px, DeviceRGB, FlateDecode

- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The risk register is compared with the agreed service level. The continuity plan is documented alongside the register of exceptions. The cloud baseline is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reconciled with the dependency map. The patch calendar is documented alongside the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The metric set is validated by the quarterly review notes. The recovery test is traced to the evidence pack held by the owner. Records are retained only as long as the schedule requires.

Plate 481

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 481 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is compared with the commissioning document. The classification scheme is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is checked against the previous year's assessment. The privileged access list is reconciled with the ticket history for the period. The control is tested at least once every twelve months.

The email authentication record is traced to the signed exception log. The backup rotation is documented alongside the approved design baseline. The endpoint baseline is reconciled with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is documented alongside the register of exceptions. The segmentation boundary is compared with the dependency map. The privileged access list is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the approved design baseline. The threat model is traced to the most recent exercise record. The privileged access list is reviewed against the commissioning document. The asset register is reviewed against the dependency map. Records are retained only as long as the schedule requires.

Plate 482

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 482 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is validated by the dependency map. The access review process is traced to the approved design baseline. The continuity plan is traced to the most recent exercise record. The mobile standard is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The endpoint baseline is documented alongside the register of exceptions. The remote access path is validated by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

124. The classification scheme

The recovery test is validated by the most recent exercise record. The encryption standard is validated by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is evidenced by the register of exceptions. The backup rotation is checked against the ticket history for the period. The asset register is traced to the previous year's assessment. The email authentication record is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

Plate 483

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 483 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is traced to the register of exceptions. The retention schedule is evidenced by the most recent exercise record. The physical controls is evidenced by the approved design baseline. The awareness cycle is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

125. The retention schedule

The remote access path is documented alongside the most recent exercise record. The vulnerability queue is checked against the quarterly review notes. The continuity plan is measured against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is validated by the register of exceptions. The endpoint baseline is measured against the quarterly review notes. The cloud baseline is evidenced by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is measured against the signed exception log. Each administrative account is checked against the signed exception log. The endpoint baseline is documented alongside the current written standard. The threat model is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 484

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 484 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is checked against the previous year's assessment. The cloud baseline is measured against the ticket history for the period. The mobile standard is evidenced by the commissioning document. The cloud baseline is reconciled with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The continuity plan is validated by the evidence pack held by the owner. The email authentication record is checked against the commissioning document. The classification scheme is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The risk register is measured against the approved design baseline. The monitoring pipeline is reviewed against the current written standard. The retention schedule is evidenced by the quarterly review notes. The patch calendar is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

Plate 485

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 485 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is checked against the register of exceptions. The classification scheme is documented alongside the ticket history for the period. Each administrative account is checked against the current written standard. The access review process is measured against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is documented alongside the register of exceptions. Every internet-facing service is traced to the approved design baseline. The hardened build is reconciled with the ticket history for the period. The mobile standard is validated by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

- Review date scheduled and visible.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

Every internet-facing service is reviewed against the register of exceptions. The asset register is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Plate 486

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 486 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reconciled with the register of exceptions. The segmentation boundary is checked against the commissioning document. The awareness cycle is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The remote access path is documented alongside the evidence pack held by the owner. Each administrative account is measured against the dependency map. The asset register is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The monitoring pipeline is checked against the signed exception log. The vendor register is traced to the agreed service level. Any deviation requires written approval and an expiry date.

The classification scheme is documented alongside the agreed service level. The cloud baseline is traced to the commissioning document. The awareness cycle is traced to the dependency map. The vulnerability queue is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is checked against the current written standard. The retention schedule is documented alongside the register of exceptions. Every internet-facing service is measured against the ticket history for the period. The privileged access list is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 487

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 487 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is measured against the most recent exercise record. The monitoring pipeline is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The continuity plan is validated by the dependency map. The privileged access list is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the agreed service level. Every internet-facing service is traced to the signed exception log. The hardened build is reviewed against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The asset register is compared with the evidence pack held by the owner. The cloud baseline is reviewed against the quarterly review notes. The third-party register is checked against the register of exceptions. The vulnerability queue is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

The patch calendar is evidenced by the register of exceptions. The access review process is validated by the quarterly review notes. The vendor register is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Plate 488

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 488 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is validated by the agreed service level. Every internet-facing service is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is compared with the register of exceptions. The segmentation boundary is checked against the current written standard. The change process is compared with the dependency map. The retention schedule is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is measured against the approved design baseline. The identity lifecycle is reconciled with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Test result attached to the record.
- Escalation path agreed with the service owner.

The email authentication record is checked against the most recent exercise record. The endpoint baseline is compared with the previous year's assessment. The continuity plan is reconciled with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Plate 489

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 489 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is measured against the most recent exercise record. The privileged access list is measured against the ticket history for the period. The remote access path is documented alongside the dependency map. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reconciled with the signed exception log. The change process is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is evidenced by the quarterly review notes. The segmentation boundary is reconciled with the approved design baseline. The cloud baseline is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The risk register is evidenced by the register of exceptions. The continuity plan is compared with the evidence pack held by the owner. The classification scheme is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is reconciled with the previous year's assessment. The vulnerability queue is evidenced by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

Plate 490

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 490 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is measured against the quarterly review notes. The continuity plan is documented alongside the previous year's assessment. The access review process is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The recovery test is reconciled with the agreed service level. The segmentation boundary is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The asset register is documented alongside the register of exceptions. The change process is checked against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The risk register is documented alongside the evidence pack held by the owner. The encryption standard is documented alongside the signed exception log. The asset register is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The third-party register is evidenced by the signed exception log. The cloud baseline is reconciled with the signed exception log. The vendor register is checked against the register of exceptions. Records are retained only as long as the schedule requires.

Plate 491

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 491 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reconciled with the current written standard. The physical controls is documented alongside the current written standard. The vendor register is compared with the signed exception log. The vendor register is validated by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is evidenced by the current written standard. The mobile standard is validated by the dependency map. The privileged access list is reconciled with the signed exception log. The retention schedule is validated by the commissioning document. Testing covers the failure case, not only the happy path.

The privileged access list is validated by the evidence pack held by the owner. The privileged access list is checked against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

Plate 492

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 492 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is traced to the agreed service level. The retention schedule is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is validated by the dependency map. The cloud baseline is reviewed against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is traced to the agreed service level. The remote access path is traced to the signed exception log. The segmentation boundary is reviewed against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The asset register is reviewed against the current written standard. The segmentation boundary is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The change process is measured against the previous year's assessment. Every internet-facing service is traced to the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Plate 493

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 493 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is evidenced by the dependency map. The vulnerability queue is evidenced by the register of exceptions. The continuity plan is measured against the most recent exercise record. The continuity plan is measured against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is validated by the commissioning document. The threat model is reviewed against the ticket history for the period. Each administrative account is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The awareness cycle is compared with the ticket history for the period. The risk register is checked against the register of exceptions. Every internet-facing service is checked against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

126. The access review process

The vulnerability queue is compared with the approved design baseline. The patch calendar is reconciled with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

Plate 494

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 494 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is checked against the ticket history for the period. The hardened build is checked against the quarterly review notes. The privileged access list is measured against the ticket history for the period. The change process is measured against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is measured against the most recent exercise record. The remote access path is checked against the agreed service level. The awareness cycle is measured against the current written standard. The identity lifecycle is reviewed against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The recovery test is evidenced by the approved design baseline. The hardened build is evidenced by the evidence pack held by the owner. The access review process is compared with the current written standard. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is checked against the current written standard. The monitoring pipeline is reviewed against the ticket history for the period. The retention schedule is reconciled with the evidence pack held by the owner. The hardened build is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

Plate 495

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 495 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is traced to the most recent exercise record. The mobile standard is validated by the approved design baseline. The identity lifecycle is compared with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is documented alongside the signed exception log. The remote access path is compared with the most recent exercise record. The threat model is documented alongside the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is checked against the dependency map. Each administrative account is reconciled with the evidence pack held by the owner. The patch calendar is checked against the agreed service level. The monitoring pipeline is validated by the previous year's assessment. The control is tested at least once every twelve months.

The vendor register is evidenced by the current written standard. The cloud baseline is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The patch calendar is measured against the quarterly review notes. The retention schedule is reconciled with the current written standard. The identity lifecycle is documented alongside the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Plate 496

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 496 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is compared with the quarterly review notes. The metric set is traced to the ticket history for the period. Every internet-facing service is measured against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

127. The threat model

The patch calendar is reviewed against the approved design baseline. The threat model is checked against the most recent exercise record. The threat model is compared with the ticket history for the period. The recovery test is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The third-party register is measured against the previous year's assessment. The hardened build is reconciled with the ticket history for the period. The physical controls is reviewed against the commissioning document. The patch calendar is compared with the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 497

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 497 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is measured against the quarterly review notes. The identity lifecycle is compared with the quarterly review notes. The control is tested at least once every twelve months.

Every internet-facing service is reviewed against the dependency map. The retention schedule is validated by the dependency map. Testing covers the failure case, not only the happy path.

The email authentication record is reconciled with the agreed service level. The asset register is measured against the ticket history for the period. The remote access path is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

The privileged access list is checked against the signed exception log. The vendor register is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

The backup rotation is reconciled with the quarterly review notes. The change process is evidenced by the most recent exercise record. The hardened build is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

Plate 498

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 498 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is validated by the signed exception log. The mobile standard is documented alongside the commissioning document. The segmentation boundary is validated by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is measured against the dependency map. The physical controls is checked against the signed exception log. The threat model is measured against the most recent exercise record. Each administrative account is traced to the signed exception log. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is traced to the current written standard. The change process is evidenced by the current written standard. The endpoint baseline is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The remote access path is validated by the previous year's assessment. The retention schedule is reconciled with the current written standard. Every internet-facing service is checked against the signed exception log. The intent is to make the safe path the default rather than an exception.

The remote access path is reconciled with the ticket history for the period. The vendor register is measured against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 499

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 499 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is documented alongside the previous year's assessment. Each administrative account is measured against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is measured against the evidence pack held by the owner. The endpoint baseline is evidenced by the evidence pack held by the owner. The metric set is documented alongside the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is compared with the approved design baseline. The access review process is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

The backup rotation is validated by the quarterly review notes. Each administrative account is documented alongside the register of exceptions. The intent is to make the safe path the default rather than an exception.

The privileged access list is traced to the approved design baseline. The asset register is reviewed against the current written standard. The endpoint baseline is documented alongside the dependency map. Any deviation requires written approval and an expiry date.

Plate 500

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 500 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is measured against the register of exceptions. The third-party register is measured against the register of exceptions. Each administrative account is validated by the current written standard. The identity lifecycle is measured against the commissioning document. The control is tested at least once every twelve months.

Every internet-facing service is compared with the agreed service level. The hardened build is traced to the register of exceptions. The encryption standard is compared with the commissioning document. The intent is to make the safe path the default rather than an exception.

The mobile standard is evidenced by the approved design baseline. The cloud baseline is documented alongside the quarterly review notes. The encryption standard is evidenced by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is reconciled with the signed exception log. The third-party register is evidenced by the commissioning document. The threat model is measured against the agreed service level. The cloud baseline is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

Plate 501

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 501 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is validated by the evidence pack held by the owner. The metric set is compared with the dependency map. The access review process is evidenced by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is measured against the most recent exercise record. The privileged access list is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

The classification scheme is reconciled with the signed exception log. The mobile standard is evidenced by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is compared with the current written standard. Each administrative account is reconciled with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The segmentation boundary is documented alongside the commissioning document. The identity lifecycle is evidenced by the most recent exercise record. The patch calendar is compared with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Plate 502

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 502 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is reviewed against the previous year's assessment. The continuity plan is reconciled with the previous year's assessment. The encryption standard is checked against the signed exception log. The third-party register is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The physical controls is documented alongside the register of exceptions. The segmentation boundary is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is compared with the ticket history for the period. The email authentication record is checked against the commissioning document. The control is tested at least once every twelve months.

The encryption standard is evidenced by the register of exceptions. The cloud baseline is reconciled with the commissioning document. The metric set is reviewed against the most recent exercise record. The metric set is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is reviewed against the most recent exercise record. The awareness cycle is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Plate 503

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 503 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is traced to the previous year's assessment. The classification scheme is evidenced by the signed exception log. The encryption standard is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Exception route documented and time-bound.

The access review process is evidenced by the commissioning document. The backup rotation is measured against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is reconciled with the agreed service level. The privileged access list is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

Plate 504

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 504 - 232 x 232 px, DeviceRGB, FlateDecode

- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The threat model is documented alongside the register of exceptions. The backup rotation is validated by the previous year's assessment. The continuity plan is checked against the previous year's assessment. The metric set is evidenced by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The mobile standard is reviewed against the evidence pack held by the owner. The continuity plan is checked against the dependency map. Metrics are reported as trends rather than single data points.

The monitoring pipeline is measured against the register of exceptions. The mobile standard is compared with the register of exceptions. Records are retained only as long as the schedule requires.

The encryption standard is checked against the dependency map. The vulnerability queue is measured against the agreed service level. Each administrative account is validated by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

Plate 505

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 505 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is reconciled with the most recent exercise record. The access review process is validated by the register of exceptions. The retention schedule is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

128. The segmentation boundary

The hardened build is traced to the signed exception log. The change process is documented alongside the current written standard. The asset register is measured against the most recent exercise record. Records are retained only as long as the schedule requires.

The continuity plan is reconciled with the most recent exercise record. The vulnerability queue is compared with the ticket history for the period. The endpoint baseline is documented alongside the agreed service level. The classification scheme is checked against the ticket history for the period. Records are retained only as long as the schedule requires.

The vendor register is compared with the ticket history for the period. The mobile standard is reconciled with the dependency map. Where automation is possible, the manual step is retained as a fallback.

Plate 506

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 506 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is reviewed against the commissioning document. The remote access path is evidenced by the evidence pack held by the owner. The third-party register is checked against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The access review process is reviewed against the previous year's assessment. The privileged access list is traced to the ticket history for the period. The control is tested at least once every twelve months.

- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Exception route documented and time-bound.

The email authentication record is compared with the quarterly review notes. The retention schedule is measured against the evidence pack held by the owner. The hardened build is measured against the approved design baseline. The hardened build is reconciled with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is reconciled with the commissioning document. The patch calendar is reviewed against the ticket history for the period. The third-party register is checked against the current written standard. The control is tested at least once every twelve months.

Plate 507

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 507 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is traced to the evidence pack held by the owner. The vendor register is validated by the previous year's assessment. The endpoint baseline is reconciled with the current written standard. Every internet-facing service is documented alongside the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is evidenced by the dependency map. The asset register is measured against the evidence pack held by the owner. The vulnerability queue is reconciled with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

129. The physical controls

The remote access path is validated by the most recent exercise record. The retention schedule is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

Every internet-facing service is checked against the register of exceptions. The retention schedule is validated by the agreed service level. The threat model is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 508

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 508 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is evidenced by the commissioning document. The asset register is reviewed against the previous year's assessment. The mobile standard is checked against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is measured against the ticket history for the period. The third-party register is validated by the evidence pack held by the owner. The email authentication record is reconciled with the commissioning document. The access review process is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is evidenced by the dependency map. The remote access path is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

130. The physical controls

The hardened build is compared with the approved design baseline. The physical controls is reviewed against the dependency map. Evidence is kept for audit, insurance and regulator requests.

Plate 509

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 509 - 232 x 232 px, DeviceRGB, FlateDecode

131. The physical controls

Every internet-facing service is validated by the quarterly review notes. The continuity plan is compared with the most recent exercise record. The identity lifecycle is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is traced to the current written standard. The third-party register is measured against the evidence pack held by the owner. The access review process is measured against the register of exceptions. The asset register is reviewed against the commissioning document. Testing covers the failure case, not only the happy path.

The classification scheme is validated by the previous year's assessment. The classification scheme is compared with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is reconciled with the approved design baseline. The retention schedule is reconciled with the previous year's assessment. The recovery test is compared with the ticket history for the period. The mobile standard is traced to the most recent exercise record. Metrics are reported as trends rather than single data points.

Plate 510

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 510 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is documented alongside the agreed service level. The mobile standard is reconciled with the ticket history for the period. The control is tested at least once every twelve months.

The patch calendar is traced to the ticket history for the period. The third-party register is checked against the dependency map. The recovery test is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reconciled with the previous year's assessment. The continuity plan is validated by the commissioning document. Every internet-facing service is traced to the current written standard. The monitoring pipeline is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Escalation path agreed with the service owner.

Plate 511

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 511 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is compared with the previous year's assessment. The awareness cycle is validated by the most recent exercise record. The segmentation boundary is compared with the previous year's assessment. The vulnerability queue is compared with the dependency map. The control is tested at least once every twelve months.

The threat model is evidenced by the quarterly review notes. The retention schedule is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is evidenced by the evidence pack held by the owner. The cloud baseline is checked against the most recent exercise record. The retention schedule is traced to the evidence pack held by the owner. The classification scheme is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

The mobile standard is measured against the approved design baseline. The change process is evidenced by the agreed service level. The vulnerability queue is reconciled with the dependency map. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is validated by the current written standard. The monitoring pipeline is evidenced by the previous year's assessment. The third-party register is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

Plate 512

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 512 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is compared with the most recent exercise record. The email authentication record is evidenced by the commissioning document. The mobile standard is documented alongside the quarterly review notes. The risk register is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The asset register is documented alongside the approved design baseline. The metric set is compared with the ticket history for the period. The remote access path is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The encryption standard is reviewed against the agreed service level. The endpoint baseline is measured against the dependency map. Testing covers the failure case, not only the happy path.

Each administrative account is reviewed against the commissioning document. The email authentication record is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

The continuity plan is evidenced by the signed exception log. The privileged access list is validated by the approved design baseline. The monitoring pipeline is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

Plate 513

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 513 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is checked against the evidence pack held by the owner. The metric set is reconciled with the previous year's assessment. The patch calendar is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The monitoring pipeline is reviewed against the commissioning document. The privileged access list is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is compared with the register of exceptions. The retention schedule is checked against the dependency map. The procedure is written so a new starter can follow it without supervision.

The vendor register is validated by the current written standard. The vendor register is documented alongside the commissioning document. The awareness cycle is traced to the quarterly review notes. The risk register is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

The vendor register is validated by the commissioning document. The physical controls is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

Plate 514

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 514 - 232 x 232 px, DeviceRGB, FlateDecode

132. The monitoring pipeline

The access review process is checked against the current written standard. The encryption standard is evidenced by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The metric set is reviewed against the previous year's assessment. The threat model is evidenced by the dependency map. The retention schedule is documented alongside the most recent exercise record. The third-party register is reviewed against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The asset register is traced to the most recent exercise record. The identity lifecycle is reviewed against the most recent exercise record. The access review process is compared with the commissioning document. The email authentication record is traced to the register of exceptions. Records are retained only as long as the schedule requires.

The third-party register is documented alongside the agreed service level. The continuity plan is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Plate 515

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 515 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is checked against the signed exception log. The cloud baseline is traced to the quarterly review notes. The mobile standard is reconciled with the most recent exercise record. The segmentation boundary is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is compared with the current written standard. Every internet-facing service is checked against the most recent exercise record. The classification scheme is traced to the commissioning document. Testing covers the failure case, not only the happy path.

The vulnerability queue is traced to the ticket history for the period. The segmentation boundary is reviewed against the most recent exercise record. The segmentation boundary is reconciled with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is documented alongside the current written standard. The asset register is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

Plate 516

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 516 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is evidenced by the approved design baseline. The third-party register is evidenced by the approved design baseline. The patch calendar is checked against the signed exception log. The access review process is validated by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The encryption standard is reconciled with the evidence pack held by the owner. The identity lifecycle is validated by the evidence pack held by the owner. Every internet-facing service is reviewed against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The vulnerability queue is checked against the approved design baseline. The vulnerability queue is traced to the agreed service level. The privileged access list is documented alongside the commissioning document. Records are retained only as long as the schedule requires.

133. The asset register

The encryption standard is measured against the commissioning document. The access review process is documented alongside the agreed service level. The awareness cycle is traced to the signed exception log. The remote access path is documented alongside the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Plate 517

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 517 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is documented alongside the evidence pack held by the owner. The email authentication record is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The access review process is checked against the register of exceptions. Every internet-facing service is checked against the ticket history for the period. The monitoring pipeline is documented alongside the signed exception log. The vendor register is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The backup rotation is reconciled with the previous year's assessment. The continuity plan is compared with the agreed service level. The patch calendar is checked against the most recent exercise record. The third-party register is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The continuity plan is checked against the quarterly review notes. The recovery test is documented alongside the dependency map. The mobile standard is measured against the signed exception log. Metrics are reported as trends rather than single data points.

Plate 518

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 518 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is traced to the commissioning document. The continuity plan is measured against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is checked against the previous year's assessment. The physical controls is checked against the dependency map. The segmentation boundary is reconciled with the previous year's assessment. Any deviation requires written approval and an expiry date.

The classification scheme is evidenced by the dependency map. The threat model is validated by the commissioning document. The awareness cycle is traced to the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is checked against the evidence pack held by the owner. The metric set is measured against the register of exceptions. The physical controls is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The cloud baseline is compared with the dependency map. The backup rotation is measured against the most recent exercise record. The cloud baseline is evidenced by the commissioning document. The awareness cycle is evidenced by the previous year's assessment. Metrics are reported as trends rather than single data points.

Plate 519

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 519 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is traced to the quarterly review notes. The awareness cycle is traced to the current written standard. The retention schedule is reviewed against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is checked against the dependency map. The retention schedule is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

134. The encryption standard

Each administrative account is reconciled with the quarterly review notes. The risk register is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

The remote access path is measured against the ticket history for the period. The privileged access list is compared with the previous year's assessment. The segmentation boundary is checked against the quarterly review notes. The threat model is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

Plate 520

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 520 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is documented alongside the approved design baseline. The privileged access list is reviewed against the dependency map. The endpoint baseline is checked against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

135. The awareness cycle

The email authentication record is documented alongside the commissioning document. The change process is compared with the dependency map. Testing covers the failure case, not only the happy path.

The identity lifecycle is documented alongside the ticket history for the period. The recovery test is reconciled with the commissioning document. The retention schedule is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is reconciled with the register of exceptions. The mobile standard is checked against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Plate 521

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 521 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is compared with the signed exception log. The remote access path is reviewed against the dependency map. The patch calendar is documented alongside the register of exceptions. The email authentication record is evidenced by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is reviewed against the evidence pack held by the owner. The encryption standard is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is checked against the approved design baseline. The physical controls is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is reconciled with the dependency map. The asset register is reconciled with the signed exception log. The cloud baseline is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is reviewed against the previous year's assessment. The retention schedule is evidenced by the current written standard. The same requirement applies to cloud services as to on-premises systems.

Plate 522

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 522 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is validated by the dependency map. The hardened build is validated by the signed exception log. The control is tested at least once every twelve months.

The vendor register is traced to the register of exceptions. The monitoring pipeline is traced to the quarterly review notes. The risk register is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The third-party register is evidenced by the previous year's assessment. The classification scheme is documented alongside the previous year's assessment. The asset register is checked against the register of exceptions. The classification scheme is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

The access review process is reviewed against the ticket history for the period. The endpoint baseline is evidenced by the agreed service level. The cloud baseline is reconciled with the commissioning document. The control is tested at least once every twelve months.

The patch calendar is compared with the agreed service level. The access review process is checked against the ticket history for the period. The cloud baseline is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

Plate 523

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 523 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is reviewed against the evidence pack held by the owner. The change process is measured against the most recent exercise record. Metrics are reported as trends rather than single data points.

The threat model is traced to the signed exception log. The metric set is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

136. The backup rotation

The vulnerability queue is reviewed against the commissioning document. The classification scheme is evidenced by the signed exception log. The privileged access list is validated by the approved design baseline. The identity lifecycle is traced to the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The change process is reconciled with the signed exception log. The encryption standard is documented alongside the current written standard. Third parties must demonstrate the control before access is granted.

The continuity plan is validated by the dependency map. The remote access path is compared with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Plate 524

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 524 - 232 x 232 px, DeviceRGB, FlateDecode

137. The remote access path

The mobile standard is reconciled with the most recent exercise record. The remote access path is compared with the approved design baseline. The backup rotation is validated by the ticket history for the period. The mobile standard is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The change process is compared with the dependency map. The continuity plan is reviewed against the quarterly review notes. The vulnerability queue is reviewed against the dependency map. The continuity plan is compared with the approved design baseline. Testing covers the failure case, not only the happy path.

The risk register is measured against the ticket history for the period. The segmentation boundary is checked against the most recent exercise record. The backup rotation is checked against the agreed service level. The remote access path is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

The risk register is reconciled with the ticket history for the period. The remote access path is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

Plate 525

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 525 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is measured against the evidence pack held by the owner. The retention schedule is documented alongside the register of exceptions. The classification scheme is reconciled with the most recent exercise record. The change process is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vendor register is measured against the commissioning document. The recovery test is compared with the evidence pack held by the owner. The remote access path is reconciled with the current written standard. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Test result attached to the record.

The mobile standard is reconciled with the register of exceptions. The monitoring pipeline is documented alongside the agreed service level. The vendor register is compared with the commissioning document. The email authentication record is compared with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Plate 526

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 526 - 232 x 232 px, DeviceRGB, FlateDecode

138. The email authentication record

The access review process is checked against the current written standard. The metric set is compared with the previous year's assessment. Every internet-facing service is traced to the previous year's assessment. The third-party register is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The recovery test is checked against the signed exception log. The awareness cycle is reviewed against the ticket history for the period. The monitoring pipeline is reviewed against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is reconciled with the most recent exercise record. The encryption standard is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

Plate 527

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 527 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is reconciled with the evidence pack held by the owner. The hardened build is traced to the current written standard. The asset register is checked against the register of exceptions. The cloud baseline is measured against the register of exceptions. The intent is to make the safe path the default rather than an exception.

139. The backup rotation

The retention schedule is documented alongside the quarterly review notes. The privileged access list is evidenced by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is validated by the ticket history for the period. The patch calendar is traced to the commissioning document. The privileged access list is compared with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is traced to the current written standard. The third-party register is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

Plate 528

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 528 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is measured against the most recent exercise record. The vendor register is reconciled with the evidence pack held by the owner. The continuity plan is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Owner named and recorded in the register.

The mobile standard is reviewed against the previous year's assessment. The access review process is compared with the signed exception log. The encryption standard is traced to the commissioning document. The change process is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The endpoint baseline is reviewed against the evidence pack held by the owner. Every internet-facing service is measured against the previous year's assessment. The retention schedule is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

Plate 529

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 529 - 232 x 232 px, DeviceRGB, FlateDecode

The hardened build is reconciled with the approved design baseline. The asset register is reviewed against the ticket history for the period. The risk register is validated by the most recent exercise record. The control is tested at least once every twelve months.

The hardened build is reviewed against the dependency map. The privileged access list is evidenced by the signed exception log. Every internet-facing service is traced to the signed exception log. The awareness cycle is measured against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is checked against the previous year's assessment. The encryption standard is documented alongside the most recent exercise record. The physical controls is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is measured against the most recent exercise record. The identity lifecycle is reviewed against the previous year's assessment. The access review process is traced to the commissioning document. The control is tested at least once every twelve months.

Plate 530

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 530 - 232 x 232 px, DeviceRGB, FlateDecode

140. The change process

The hardened build is traced to the approved design baseline. Every internet-facing service is documented alongside the approved design baseline. The classification scheme is evidenced by the approved design baseline. The vendor register is checked against the commissioning document. Metrics are reported as trends rather than single data points.

The vulnerability queue is compared with the most recent exercise record. The change process is measured against the commissioning document. The awareness cycle is validated by the most recent exercise record. The control is tested at least once every twelve months.

The hardened build is reconciled with the ticket history for the period. The identity lifecycle is reconciled with the previous year's assessment. The email authentication record is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is reconciled with the signed exception log. The identity lifecycle is reconciled with the current written standard. The encryption standard is measured against the signed exception log. The vendor register is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

Plate 531

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 531 - 232 x 232 px, DeviceRGB, FlateDecode

The change process is reconciled with the previous year's assessment. The hardened build is reviewed against the current written standard. The hardened build is reviewed against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is traced to the approved design baseline. The retention schedule is reviewed against the agreed service level. The remote access path is compared with the current written standard. The continuity plan is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

- Backup of the change retained for rollback.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Exception route documented and time-bound.

The endpoint baseline is documented alongside the current written standard. The recovery test is measured against the register of exceptions. Records are retained only as long as the schedule requires.

Plate 532

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 532 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is measured against the evidence pack held by the owner. The vendor register is reconciled with the dependency map. The recovery test is traced to the quarterly review notes. The cloud baseline is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

141. The endpoint baseline

The backup rotation is documented alongside the commissioning document. The retention schedule is reconciled with the ticket history for the period. The recovery test is reviewed against the commissioning document. The hardened build is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The patch calendar is reviewed against the ticket history for the period. The threat model is traced to the most recent exercise record. The email authentication record is checked against the current written standard. The threat model is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Plate 533

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 533 - 232 x 232 px, DeviceRGB, FlateDecode

- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Notification list confirmed before execution.

The cloud baseline is documented alongside the register of exceptions. Every internet-facing service is traced to the agreed service level. The change process is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The mobile standard is compared with the dependency map. The risk register is measured against the quarterly review notes. The monitoring pipeline is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is validated by the commissioning document. The risk register is checked against the register of exceptions. The access review process is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Plate 534

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 534 - 232 x 232 px, DeviceRGB, FlateDecode

The risk register is documented alongside the quarterly review notes. The asset register is measured against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is evidenced by the signed exception log. The change process is traced to the approved design baseline. The risk register is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

The physical controls is compared with the quarterly review notes. The email authentication record is validated by the register of exceptions. The continuity plan is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

The retention schedule is validated by the evidence pack held by the owner. The awareness cycle is reconciled with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is evidenced by the evidence pack held by the owner. The change process is evidenced by the evidence pack held by the owner. The metric set is documented alongside the quarterly review notes. The intent is to make the safe path the default rather than an exception.

Plate 535

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 535 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the evidence pack held by the owner. The privileged access list is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The hardened build is validated by the approved design baseline. The remote access path is checked against the dependency map. The access review process is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The retention schedule is documented alongside the previous year's assessment. The encryption standard is reviewed against the dependency map. The monitoring pipeline is traced to the current written standard. Records are retained only as long as the schedule requires.

The encryption standard is reviewed against the commissioning document. Each administrative account is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The retention schedule is traced to the most recent exercise record. The encryption standard is documented alongside the commissioning document. The hardened build is compared with the register of exceptions. Any deviation requires written approval and an expiry date.

Plate 536

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 536 - 232 x 232 px, DeviceRGB, FlateDecode

- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.

The retention schedule is compared with the quarterly review notes. The vulnerability queue is evidenced by the register of exceptions. The classification scheme is traced to the most recent exercise record. Testing covers the failure case, not only the happy path.

Each administrative account is measured against the signed exception log. The risk register is validated by the approved design baseline. The continuity plan is evidenced by the previous year's assessment. The identity lifecycle is checked against the dependency map. Metrics are reported as trends rather than single data points.

The change process is documented alongside the most recent exercise record. The cloud baseline is documented alongside the quarterly review notes. The risk register is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The change process is documented alongside the commissioning document. The endpoint baseline is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

Plate 537

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 537 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is validated by the evidence pack held by the owner. Each administrative account is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is validated by the most recent exercise record. The endpoint baseline is evidenced by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is checked against the current written standard. The asset register is reviewed against the commissioning document. Testing covers the failure case, not only the happy path.

The access review process is reviewed against the approved design baseline. The retention schedule is measured against the current written standard. The control is tested at least once every twelve months.

The privileged access list is checked against the previous year's assessment. The recovery test is checked against the evidence pack held by the owner. The third-party register is documented alongside the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Plate 538

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 538 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is measured against the register of exceptions. The monitoring pipeline is compared with the approved design baseline. The identity lifecycle is reviewed against the commissioning document. The retention schedule is checked against the current written standard. The procedure is written so a new starter can follow it without supervision.

The risk register is validated by the quarterly review notes. The segmentation boundary is validated by the signed exception log. The endpoint baseline is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The cloud baseline is measured against the signed exception log. The continuity plan is traced to the previous year's assessment. The vendor register is evidenced by the signed exception log. The retention schedule is traced to the current written standard. The control is tested at least once every twelve months.

Every internet-facing service is traced to the agreed service level. The awareness cycle is compared with the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 539

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 539 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is reviewed against the current written standard. The privileged access list is reviewed against the dependency map. The privileged access list is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is documented alongside the signed exception log. The backup rotation is validated by the dependency map. The asset register is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is validated by the dependency map. The physical controls is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The third-party register is reviewed against the signed exception log. The recovery test is validated by the commissioning document. The threat model is traced to the agreed service level. The control is tested at least once every twelve months.

The access review process is compared with the register of exceptions. Every internet-facing service is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

Plate 540

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 540 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is measured against the commissioning document. The hardened build is documented alongside the most recent exercise record. The backup rotation is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

The awareness cycle is documented alongside the agreed service level. The change process is traced to the current written standard. The threat model is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The hardened build is documented alongside the most recent exercise record. The identity lifecycle is compared with the evidence pack held by the owner. The classification scheme is evidenced by the current written standard. The cloud baseline is validated by the register of exceptions. Metrics are reported as trends rather than single data points.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

Plate 541

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 541 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is checked against the most recent exercise record. The recovery test is reviewed against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is documented alongside the current written standard. The metric set is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The third-party register is compared with the commissioning document. The vendor register is reviewed against the most recent exercise record. The threat model is documented alongside the agreed service level. The third-party register is compared with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

142. Every internet-facing service

The monitoring pipeline is documented alongside the evidence pack held by the owner. The backup rotation is traced to the ticket history for the period. The mobile standard is reconciled with the ticket history for the period. The recovery test is reviewed against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Plate 542

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 542 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is reconciled with the commissioning document. The continuity plan is evidenced by the evidence pack held by the owner. The change process is validated by the dependency map. The threat model is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The endpoint baseline is compared with the commissioning document. The hardened build is evidenced by the commissioning document. The email authentication record is documented alongside the most recent exercise record. The cloud baseline is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The access review process is traced to the agreed service level. The recovery test is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is reconciled with the agreed service level. The endpoint baseline is evidenced by the dependency map. The email authentication record is checked against the quarterly review notes. The patch calendar is reviewed against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 543

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 543 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is documented alongside the approved design baseline. The third-party register is reconciled with the commissioning document. The control is tested at least once every twelve months.

The remote access path is compared with the commissioning document. Every internet-facing service is reconciled with the quarterly review notes. Any deviation requires written approval and an expiry date.

Every internet-facing service is reconciled with the ticket history for the period. The classification scheme is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is reviewed against the ticket history for the period. The risk register is validated by the agreed service level. The metric set is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

The classification scheme is reviewed against the previous year's assessment. The encryption standard is reconciled with the signed exception log. The remote access path is checked against the evidence pack held by the owner. The cloud baseline is validated by the previous year's assessment. The control is tested at least once every twelve months.

Plate 544

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 544 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is traced to the current written standard. The third-party register is reconciled with the previous year's assessment. The vulnerability queue is documented alongside the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is reviewed against the agreed service level. The threat model is traced to the signed exception log. The third-party register is evidenced by the agreed service level. The identity lifecycle is reviewed against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The patch calendar is reconciled with the previous year's assessment. The segmentation boundary is compared with the signed exception log. The physical controls is reconciled with the signed exception log. Metrics are reported as trends rather than single data points.

The endpoint baseline is reconciled with the signed exception log. The metric set is reviewed against the evidence pack held by the owner. The access review process is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 545

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 545 - 232 x 232 px, DeviceRGB, FlateDecode

The recovery test is documented alongside the previous year's assessment. The patch calendar is reviewed against the approved design baseline. The threat model is compared with the dependency map. The physical controls is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The threat model is evidenced by the evidence pack held by the owner. The backup rotation is checked against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is traced to the commissioning document. The segmentation boundary is validated by the previous year's assessment. The asset register is reviewed against the dependency map. The awareness cycle is traced to the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is measured against the current written standard. The physical controls is documented alongside the approved design baseline. The awareness cycle is reviewed against the register of exceptions. The awareness cycle is traced to the dependency map. Any deviation requires written approval and an expiry date.

Plate 546

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 546 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is measured against the previous year's assessment. The endpoint baseline is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

Each administrative account is documented alongside the approved design baseline. The identity lifecycle is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

143. The metric set

The segmentation boundary is evidenced by the signed exception log. The change process is evidenced by the register of exceptions. The physical controls is evidenced by the ticket history for the period. Any deviation requires written approval and an expiry date.

144. The endpoint baseline

The vulnerability queue is measured against the commissioning document. The identity lifecycle is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Plate 547

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 547 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is validated by the most recent exercise record. The access review process is reconciled with the register of exceptions. The access review process is checked against the approved design baseline. Testing covers the failure case, not only the happy path.

The endpoint baseline is validated by the commissioning document. The monitoring pipeline is traced to the commissioning document. The retention schedule is compared with the agreed service level. Every internet-facing service is compared with the dependency map. Records are retained only as long as the schedule requires.

The access review process is traced to the dependency map. The identity lifecycle is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The remote access path is evidenced by the approved design baseline. The mobile standard is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The access review process is checked against the register of exceptions. The access review process is validated by the dependency map. The cloud baseline is checked against the current written standard. Testing covers the failure case, not only the happy path.

Plate 548

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 548 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is reconciled with the commissioning document. The email authentication record is evidenced by the ticket history for the period. The mobile standard is documented alongside the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is validated by the current written standard. The metric set is documented alongside the most recent exercise record. The monitoring pipeline is reconciled with the current written standard. The asset register is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The access review process is measured against the most recent exercise record. The encryption standard is reviewed against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The encryption standard is traced to the most recent exercise record. The third-party register is checked against the register of exceptions. The patch calendar is reviewed against the quarterly review notes. The third-party register is validated by the agreed service level. The control is tested at least once every twelve months.

Plate 549

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 549 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is documented alongside the approved design baseline. The classification scheme is evidenced by the dependency map. The hardened build is reviewed against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The asset register is traced to the quarterly review notes. The access review process is reconciled with the evidence pack held by the owner. The third-party register is evidenced by the current written standard. The third-party register is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

145. The metric set

The access review process is documented alongside the signed exception log. Each administrative account is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The classification scheme is documented alongside the previous year's assessment. The backup rotation is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

Plate 550

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 550 - 232 x 232 px, DeviceRGB, FlateDecode

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.

The email authentication record is compared with the most recent exercise record. The identity lifecycle is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is measured against the approved design baseline. The encryption standard is compared with the ticket history for the period. The change process is measured against the register of exceptions. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the previous year's assessment. The access review process is documented alongside the dependency map. The cloud baseline is checked against the most recent exercise record. The control is tested at least once every twelve months.

The vendor register is reconciled with the quarterly review notes. The cloud baseline is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

Plate 551

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 551 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is traced to the ticket history for the period. The third-party register is traced to the previous year's assessment. Each administrative account is validated by the most recent exercise record. The recovery test is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The recovery test is reconciled with the current written standard. The remote access path is checked against the most recent exercise record. The change process is traced to the agreed service level. Records are retained only as long as the schedule requires.

146. The remote access path

The privileged access list is evidenced by the commissioning document. The identity lifecycle is evidenced by the quarterly review notes. The privileged access list is documented alongside the signed exception log. Metrics are reported as trends rather than single data points.

The classification scheme is evidenced by the commissioning document. The change process is compared with the previous year's assessment. The mobile standard is checked against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

Plate 552

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 552 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is traced to the agreed service level. The third-party register is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

147. Every internet-facing service

The retention schedule is evidenced by the ticket history for the period. Every internet-facing service is reviewed against the agreed service level. The access review process is measured against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is reconciled with the register of exceptions. The email authentication record is checked against the commissioning document. The awareness cycle is checked against the previous year's assessment. Third parties must demonstrate the control before access is granted.

- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.

Plate 553

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 553 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is documented alongside the register of exceptions. The access review process is reconciled with the quarterly review notes. The patch calendar is measured against the most recent exercise record. The backup rotation is traced to the most recent exercise record. The control is tested at least once every twelve months.

The asset register is reviewed against the current written standard. The risk register is validated by the register of exceptions. The identity lifecycle is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is validated by the signed exception log. The email authentication record is reviewed against the quarterly review notes. Each administrative account is traced to the signed exception log. The control is tested at least once every twelve months.

The physical controls is documented alongside the ticket history for the period. The risk register is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the commissioning document. The cloud baseline is traced to the quarterly review notes. The backup rotation is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Plate 554

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 554 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is documented alongside the commissioning document. Each administrative account is measured against the approved design baseline. The encryption standard is measured against the commissioning document. The hardened build is evidenced by the register of exceptions. The control is tested at least once every twelve months.

The remote access path is reviewed against the approved design baseline. The privileged access list is reconciled with the approved design baseline. The email authentication record is compared with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is reviewed against the current written standard. The physical controls is reviewed against the dependency map. The recovery test is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is documented alongside the register of exceptions. Each administrative account is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

Every internet-facing service is traced to the ticket history for the period. Every internet-facing service is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Plate 555

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 555 - 232 x 232 px, DeviceRGB, FlateDecode

- Test result attached to the record.
- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The risk register is documented alongside the previous year's assessment. The encryption standard is reconciled with the quarterly review notes. Records are retained only as long as the schedule requires.

The segmentation boundary is validated by the commissioning document. The vendor register is reconciled with the approved design baseline. The change process is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

Plate 556

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 556 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is traced to the register of exceptions. The risk register is compared with the signed exception log. The awareness cycle is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The change process is evidenced by the commissioning document. The change process is evidenced by the register of exceptions. Third parties must demonstrate the control before access is granted.

The recovery test is evidenced by the quarterly review notes. The classification scheme is documented alongside the signed exception log. The segmentation boundary is reviewed against the current written standard. Third parties must demonstrate the control before access is granted.

The continuity plan is traced to the register of exceptions. The recovery test is reviewed against the quarterly review notes. The awareness cycle is checked against the dependency map. The mobile standard is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is traced to the evidence pack held by the owner. The endpoint baseline is reviewed against the approved design baseline. The recovery test is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

Plate 557

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 557 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is compared with the commissioning document. The continuity plan is validated by the dependency map. Testing covers the failure case, not only the happy path.

Every internet-facing service is measured against the evidence pack held by the owner. The backup rotation is evidenced by the quarterly review notes. The risk register is validated by the register of exceptions. Every internet-facing service is reconciled with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is evidenced by the register of exceptions. The identity lifecycle is compared with the agreed service level. The vulnerability queue is reconciled with the register of exceptions. The awareness cycle is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is documented alongside the previous year's assessment. The cloud baseline is evidenced by the dependency map. Testing covers the failure case, not only the happy path.

Plate 558

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 558 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is evidenced by the signed exception log. The access review process is validated by the ticket history for the period. The encryption standard is documented alongside the approved design baseline. The awareness cycle is validated by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is evidenced by the agreed service level. The monitoring pipeline is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is measured against the ticket history for the period. The cloud baseline is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The hardened build is documented alongside the register of exceptions. The risk register is measured against the commissioning document. The risk register is reconciled with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is reconciled with the quarterly review notes. The hardened build is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

Plate 559

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 559 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is validated by the quarterly review notes. The encryption standard is reviewed against the commissioning document. The risk register is validated by the ticket history for the period. The classification scheme is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is compared with the ticket history for the period. The classification scheme is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is reconciled with the commissioning document. The privileged access list is measured against the dependency map. The vendor register is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is measured against the most recent exercise record. The patch calendar is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Plate 560

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 560 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is compared with the approved design baseline. The metric set is traced to the evidence pack held by the owner. The identity lifecycle is reviewed against the commissioning document. Metrics are reported as trends rather than single data points.

The mobile standard is evidenced by the previous year's assessment. The cloud baseline is documented alongside the ticket history for the period. The vulnerability queue is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is reconciled with the evidence pack held by the owner. The retention schedule is validated by the dependency map. The third-party register is checked against the dependency map. The retention schedule is validated by the commissioning document. Evidence is kept for audit, insurance and regulator requests.

148. The awareness cycle

The threat model is measured against the quarterly review notes. The mobile standard is compared with the evidence pack held by the owner. The retention schedule is reconciled with the dependency map. The threat model is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Plate 561

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 561 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is traced to the evidence pack held by the owner. The endpoint baseline is validated by the signed exception log. The endpoint baseline is reconciled with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is compared with the signed exception log. The metric set is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is documented alongside the register of exceptions. The awareness cycle is measured against the most recent exercise record. The hardened build is validated by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The asset register is reviewed against the evidence pack held by the owner. The cloud baseline is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

149. The vulnerability queue

The hardened build is traced to the evidence pack held by the owner. The risk register is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 562

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 562 - 232 x 232 px, DeviceRGB, FlateDecode

150. The privileged access list

The patch calendar is checked against the commissioning document. The retention schedule is compared with the approved design baseline. The privileged access list is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is checked against the quarterly review notes. The remote access path is measured against the previous year's assessment. The vulnerability queue is reviewed against the ticket history for the period. The vulnerability queue is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is evidenced by the commissioning document. Every internet-facing service is validated by the most recent exercise record. The monitoring pipeline is traced to the quarterly review notes. The threat model is compared with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is documented alongside the current written standard. The retention schedule is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 563

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 563 - 232 x 232 px, DeviceRGB, FlateDecode

The mobile standard is checked against the signed exception log. The retention schedule is reviewed against the agreed service level. The vulnerability queue is evidenced by the agreed service level. The control is tested at least once every twelve months.

The access review process is reconciled with the approved design baseline. The vendor register is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the dependency map. The risk register is reviewed against the dependency map. The email authentication record is reconciled with the quarterly review notes. The mobile standard is reconciled with the current written standard. Records are retained only as long as the schedule requires.

The awareness cycle is reviewed against the ticket history for the period. The remote access path is reconciled with the register of exceptions. The vulnerability queue is checked against the current written standard. Metrics are reported as trends rather than single data points.

The cloud baseline is traced to the commissioning document. The segmentation boundary is traced to the commissioning document. The risk register is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

Plate 564

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 564 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is checked against the quarterly review notes. The email authentication record is checked against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.

The endpoint baseline is reviewed against the current written standard. The endpoint baseline is compared with the register of exceptions. The recovery test is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The continuity plan is documented alongside the dependency map. The segmentation boundary is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The metric set is evidenced by the quarterly review notes. The vulnerability queue is checked against the current written standard. The backup rotation is evidenced by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

Plate 565

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 565 - 232 x 232 px, DeviceRGB, FlateDecode

151. The mobile standard

The cloud baseline is traced to the ticket history for the period. The classification scheme is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is measured against the most recent exercise record. The remote access path is measured against the approved design baseline. The classification scheme is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is compared with the previous year's assessment. The mobile standard is documented alongside the ticket history for the period. The threat model is traced to the commissioning document. The email authentication record is documented alongside the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is checked against the evidence pack held by the owner. The monitoring pipeline is validated by the agreed service level. The patch calendar is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

Plate 566

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 566 - 232 x 232 px, DeviceRGB, FlateDecode

The physical controls is evidenced by the dependency map. The third-party register is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The change process is reconciled with the evidence pack held by the owner. Every internet-facing service is traced to the ticket history for the period. The access review process is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reconciled with the commissioning document. The risk register is documented alongside the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is validated by the evidence pack held by the owner. Each administrative account is compared with the register of exceptions. The remote access path is reconciled with the register of exceptions. The recovery test is validated by the commissioning document. Metrics are reported as trends rather than single data points.

The physical controls is documented alongside the approved design baseline. The privileged access list is measured against the evidence pack held by the owner. The retention schedule is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

Plate 567

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 567 - 232 x 232 px, DeviceRGB, FlateDecode

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Notification list confirmed before execution.

The threat model is reconciled with the current written standard. The segmentation boundary is reviewed against the current written standard. The access review process is documented alongside the agreed service level. The threat model is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is validated by the approved design baseline. The email authentication record is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

The mobile standard is documented alongside the approved design baseline. The metric set is validated by the register of exceptions. Each administrative account is measured against the most recent exercise record. The recovery test is documented alongside the quarterly review notes. The control is tested at least once every twelve months.

Plate 568

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 568 - 232 x 232 px, DeviceRGB, FlateDecode

The endpoint baseline is compared with the commissioning document. The monitoring pipeline is compared with the current written standard. The access review process is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

The awareness cycle is evidenced by the evidence pack held by the owner. The hardened build is evidenced by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the evidence pack held by the owner. Every internet-facing service is compared with the commissioning document. The metric set is reconciled with the signed exception log. The endpoint baseline is measured against the dependency map. The control is tested at least once every twelve months.

The physical controls is compared with the dependency map. The continuity plan is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 569

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 569 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is checked against the current written standard. The cloud baseline is measured against the signed exception log. The metric set is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is compared with the dependency map. Each administrative account is checked against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is validated by the previous year's assessment. The privileged access list is evidenced by the dependency map. The mobile standard is documented alongside the current written standard. The recovery test is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

The asset register is reviewed against the register of exceptions. The continuity plan is checked against the register of exceptions. The asset register is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

Plate 570

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 570 - 232 x 232 px, DeviceRGB, FlateDecode

The access review process is evidenced by the evidence pack held by the owner. The physical controls is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is documented alongside the quarterly review notes. The monitoring pipeline is validated by the dependency map. The change process is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The awareness cycle is measured against the agreed service level. The threat model is compared with the dependency map. The access review process is validated by the commissioning document. Each administrative account is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Plate 571

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 571 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is measured against the previous year's assessment. The mobile standard is evidenced by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is validated by the approved design baseline. The cloud baseline is compared with the quarterly review notes. Each administrative account is validated by the dependency map. Third parties must demonstrate the control before access is granted.

- Owner named and recorded in the register.
- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.

The awareness cycle is traced to the evidence pack held by the owner. The cloud baseline is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is validated by the current written standard. The endpoint baseline is measured against the dependency map. The segmentation boundary is documented alongside the register of exceptions. The vendor register is compared with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

Plate 572

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 572 - 232 x 232 px, DeviceRGB, FlateDecode

152. The privileged access list

The endpoint baseline is checked against the evidence pack held by the owner. The identity lifecycle is validated by the current written standard. The risk register is validated by the agreed service level. The monitoring pipeline is reconciled with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is reconciled with the most recent exercise record. The patch calendar is checked against the approved design baseline. The awareness cycle is reconciled with the approved design baseline. The cloud baseline is measured against the dependency map. Any deviation requires written approval and an expiry date.

The threat model is measured against the signed exception log. The awareness cycle is validated by the commissioning document. The continuity plan is evidenced by the ticket history for the period. Testing covers the failure case, not only the happy path.

The privileged access list is validated by the agreed service level. The identity lifecycle is reconciled with the ticket history for the period. The physical controls is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

Plate 573

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 573 - 232 x 232 px, DeviceRGB, FlateDecode

Each administrative account is checked against the agreed service level. The email authentication record is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is measured against the commissioning document. The access review process is checked against the signed exception log. The metric set is evidenced by the commissioning document. The change process is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

The retention schedule is checked against the ticket history for the period. The threat model is reconciled with the previous year's assessment. The endpoint baseline is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

The classification scheme is documented alongside the ticket history for the period. The vulnerability queue is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is reconciled with the signed exception log. The endpoint baseline is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

Plate 574

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 574 - 232 x 232 px, DeviceRGB, FlateDecode

The continuity plan is checked against the quarterly review notes. The patch calendar is reconciled with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is validated by the signed exception log. The cloud baseline is validated by the quarterly review notes. The encryption standard is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The change process is compared with the dependency map. The threat model is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is documented alongside the approved design baseline. The threat model is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

Each administrative account is measured against the agreed service level. The endpoint baseline is measured against the ticket history for the period. The backup rotation is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is reconciled with the ticket history for the period. The backup rotation is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

Plate 575

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 575 - 232 x 232 px, DeviceRGB, FlateDecode

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.

The hardened build is validated by the dependency map. The access review process is traced to the current written standard. Testing covers the failure case, not only the happy path.

The asset register is documented alongside the previous year's assessment. The vulnerability queue is evidenced by the signed exception log. The physical controls is checked against the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is traced to the agreed service level. The remote access path is measured against the dependency map. Testing covers the failure case, not only the happy path.

The continuity plan is checked against the dependency map. The monitoring pipeline is validated by the commissioning document. The encryption standard is reconciled with the agreed service level. The control is tested at least once every twelve months.

Plate 576

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 576 - 232 x 232 px, DeviceRGB, FlateDecode

The metric set is checked against the agreed service level. The hardened build is measured against the dependency map. The access review process is measured against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The access review process is checked against the dependency map. The asset register is documented alongside the current written standard. The vendor register is evidenced by the dependency map. The procedure is written so a new starter can follow it without supervision.

The encryption standard is traced to the agreed service level. The segmentation boundary is traced to the agreed service level. The encryption standard is compared with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is compared with the current written standard. The backup rotation is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is validated by the most recent exercise record. The risk register is validated by the approved design baseline. The asset register is measured against the approved design baseline. The awareness cycle is reconciled with the commissioning document. Testing covers the failure case, not only the happy path.

Plate 577

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 577 - 232 x 232 px, DeviceRGB, FlateDecode

153. The physical controls

Every internet-facing service is reconciled with the quarterly review notes. The change process is checked against the previous year's assessment. The continuity plan is checked against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is reviewed against the most recent exercise record. Each administrative account is reviewed against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is checked against the previous year's assessment. The recovery test is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.

Plate 578

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 578 - 232 x 232 px, DeviceRGB, FlateDecode

The asset register is documented alongside the dependency map. The awareness cycle is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is measured against the signed exception log. The change process is documented alongside the most recent exercise record. The backup rotation is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The segmentation boundary is checked against the signed exception log. The recovery test is reconciled with the commissioning document. The patch calendar is reconciled with the ticket history for the period. The control is tested at least once every twelve months.

The encryption standard is checked against the ticket history for the period. The endpoint baseline is validated by the previous year's assessment. The awareness cycle is validated by the signed exception log. The control is tested at least once every twelve months.

The privileged access list is reconciled with the register of exceptions. The vendor register is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Plate 579

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 579 - 232 x 232 px, DeviceRGB, FlateDecode

Every internet-facing service is compared with the most recent exercise record. The retention schedule is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is checked against the agreed service level. The hardened build is documented alongside the signed exception log. The classification scheme is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The metric set is validated by the most recent exercise record. Each administrative account is evidenced by the most recent exercise record. The vulnerability queue is compared with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is evidenced by the dependency map. The vulnerability queue is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The third-party register is validated by the evidence pack held by the owner. The email authentication record is measured against the previous year's assessment. The threat model is reconciled with the current written standard. The continuity plan is compared with the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Plate 580

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 580 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is reviewed against the signed exception log. The vendor register is documented alongside the evidence pack held by the owner. The threat model is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is reconciled with the agreed service level. The threat model is compared with the current written standard. The threat model is reconciled with the most recent exercise record. The third-party register is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

Each administrative account is measured against the approved design baseline. The vendor register is traced to the commissioning document. The third-party register is reconciled with the dependency map. The privileged access list is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is documented alongside the approved design baseline. The continuity plan is evidenced by the signed exception log. The risk register is validated by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

Plate 581

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 581 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is reconciled with the previous year's assessment. Every internet-facing service is evidenced by the evidence pack held by the owner. The risk register is compared with the commissioning document. The mobile standard is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is compared with the quarterly review notes. The segmentation boundary is reconciled with the approved design baseline. The metric set is reviewed against the agreed service level. The patch calendar is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The hardened build is validated by the quarterly review notes. The encryption standard is reviewed against the signed exception log. The endpoint baseline is evidenced by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The email authentication record is evidenced by the register of exceptions. The vulnerability queue is documented alongside the agreed service level. The asset register is validated by the agreed service level. Every internet-facing service is traced to the dependency map. Testing covers the failure case, not only the happy path.

Plate 582

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 582 - 232 x 232 px, DeviceRGB, FlateDecode

The identity lifecycle is reviewed against the commissioning document. The cloud baseline is checked against the most recent exercise record. The hardened build is reconciled with the register of exceptions. The hardened build is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The recovery test is documented alongside the register of exceptions. The third-party register is measured against the agreed service level. Each administrative account is compared with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is validated by the most recent exercise record. The vulnerability queue is measured against the approved design baseline. The remote access path is compared with the evidence pack held by the owner. The email authentication record is validated by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is measured against the signed exception log. The awareness cycle is traced to the most recent exercise record. The vendor register is traced to the evidence pack held by the owner. The asset register is traced to the commissioning document. The control is tested at least once every twelve months.

Plate 583

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 583 - 232 x 232 px, DeviceRGB, FlateDecode

The retention schedule is measured against the dependency map. The awareness cycle is documented alongside the commissioning document. The segmentation boundary is checked against the current written standard. The identity lifecycle is documented alongside the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

154. The recovery test

Every internet-facing service is documented alongside the ticket history for the period. The threat model is checked against the dependency map. The remote access path is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

155. Every internet-facing service

The awareness cycle is reconciled with the ticket history for the period. The continuity plan is evidenced by the signed exception log. The continuity plan is measured against the register of exceptions. The asset register is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Plate 584

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 584 - 232 x 232 px, DeviceRGB, FlateDecode

The encryption standard is reconciled with the most recent exercise record. The threat model is measured against the evidence pack held by the owner. The awareness cycle is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is validated by the most recent exercise record. The cloud baseline is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

The endpoint baseline is checked against the approved design baseline. The vendor register is evidenced by the current written standard. The physical controls is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The continuity plan is traced to the register of exceptions. The vulnerability queue is reconciled with the quarterly review notes. The awareness cycle is evidenced by the most recent exercise record. The asset register is evidenced by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 585

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 585 - 232 x 232 px, DeviceRGB, FlateDecode

The privileged access list is documented alongside the most recent exercise record. The risk register is checked against the evidence pack held by the owner. The cloud baseline is reconciled with the ticket history for the period. The third-party register is compared with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The asset register is validated by the agreed service level. The cloud baseline is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

The backup rotation is evidenced by the approved design baseline. The identity lifecycle is validated by the approved design baseline. The hardened build is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is evidenced by the current written standard. The classification scheme is evidenced by the signed exception log. The segmentation boundary is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The encryption standard is reviewed against the register of exceptions. The recovery test is reconciled with the quarterly review notes. The physical controls is evidenced by the evidence pack held by the owner. The mobile standard is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

Plate 586

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 586 - 232 x 232 px, DeviceRGB, FlateDecode

The threat model is reconciled with the dependency map. The retention schedule is measured against the most recent exercise record. The control is tested at least once every twelve months.

The patch calendar is compared with the approved design baseline. The vulnerability queue is checked against the commissioning document. The awareness cycle is documented alongside the agreed service level. The intent is to make the safe path the default rather than an exception.

- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The cloud baseline is reviewed against the commissioning document. The backup rotation is compared with the ticket history for the period. The continuity plan is reviewed against the approved design baseline. The continuity plan is reviewed against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Plate 587

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 587 - 232 x 232 px, DeviceRGB, FlateDecode

The remote access path is validated by the dependency map. The metric set is checked against the approved design baseline. The backup rotation is evidenced by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is validated by the evidence pack held by the owner. The monitoring pipeline is validated by the ticket history for the period. The change process is evidenced by the evidence pack held by the owner. The metric set is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

The patch calendar is checked against the register of exceptions. The monitoring pipeline is evidenced by the previous year's assessment. The monitoring pipeline is reviewed against the signed exception log. The control is tested at least once every twelve months.

The physical controls is traced to the agreed service level. The hardened build is evidenced by the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The remote access path is validated by the evidence pack held by the owner. The mobile standard is evidenced by the agreed service level. Each administrative account is validated by the dependency map. The control is tested at least once every twelve months.

Plate 588

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 588 - 232 x 232 px, DeviceRGB, FlateDecode

156. The patch calendar

The backup rotation is compared with the approved design baseline. The third-party register is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.

The endpoint baseline is validated by the dependency map. The encryption standard is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The asset register is reviewed against the register of exceptions. The asset register is reviewed against the dependency map. The awareness cycle is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Plate 589

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 589 - 232 x 232 px, DeviceRGB, FlateDecode

The backup rotation is checked against the register of exceptions. The hardened build is reconciled with the signed exception log. Every internet-facing service is checked against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The hardened build is compared with the signed exception log. The mobile standard is checked against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is documented alongside the signed exception log. The asset register is evidenced by the ticket history for the period. The hardened build is validated by the current written standard. Metrics are reported as trends rather than single data points.

The access review process is reconciled with the most recent exercise record. The privileged access list is validated by the register of exceptions. The cloud baseline is compared with the register of exceptions. The cloud baseline is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

The asset register is reconciled with the register of exceptions. The cloud baseline is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Plate 590

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 590 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is evidenced by the most recent exercise record. The email authentication record is validated by the signed exception log. The privileged access list is measured against the agreed service level. The backup rotation is validated by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is traced to the quarterly review notes. The patch calendar is compared with the quarterly review notes. The mobile standard is checked against the commissioning document. The segmentation boundary is compared with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The physical controls is checked against the current written standard. The remote access path is traced to the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The recovery test is checked against the agreed service level. The asset register is measured against the dependency map. The identity lifecycle is reconciled with the commissioning document. The monitoring pipeline is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Plate 591

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 591 - 232 x 232 px, DeviceRGB, FlateDecode

The cloud baseline is documented alongside the evidence pack held by the owner. The patch calendar is evidenced by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The change process is traced to the quarterly review notes. The change process is compared with the current written standard. The remote access path is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is reviewed against the approved design baseline. The privileged access list is checked against the approved design baseline. The hardened build is validated by the previous year's assessment. The hardened build is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is compared with the signed exception log. The monitoring pipeline is checked against the signed exception log. The classification scheme is traced to the signed exception log. The classification scheme is compared with the signed exception log. Records are retained only as long as the schedule requires.

Plate 592

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 592 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is measured against the previous year's assessment. The asset register is validated by the register of exceptions. The continuity plan is evidenced by the dependency map. The hardened build is evidenced by the quarterly review notes. Any deviation requires written approval and an expiry date.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.

157. The threat model

The hardened build is documented alongside the approved design baseline. The recovery test is compared with the approved design baseline. The vendor register is measured against the previous year's assessment. The recovery test is compared with the current written standard. Evidence is kept for audit, insurance and regulator requests.

Plate 593

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 593 - 232 x 232 px, DeviceRGB, FlateDecode

158. The retention schedule

The metric set is compared with the ticket history for the period. The third-party register is compared with the register of exceptions. The patch calendar is traced to the most recent exercise record. The risk register is reviewed against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is validated by the previous year's assessment. The continuity plan is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is traced to the commissioning document. The change process is validated by the agreed service level. Records are retained only as long as the schedule requires.

Plate 594

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 594 - 232 x 232 px, DeviceRGB, FlateDecode

The classification scheme is validated by the current written standard. The mobile standard is validated by the most recent exercise record. The identity lifecycle is documented alongside the evidence pack held by the owner. The monitoring pipeline is documented alongside the commissioning document. The control is tested at least once every twelve months.

The vulnerability queue is documented alongside the most recent exercise record. The encryption standard is checked against the current written standard. The hardened build is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The recovery test is documented alongside the quarterly review notes. The cloud baseline is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is measured against the previous year's assessment. The monitoring pipeline is validated by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

Plate 595

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 595 - 232 x 232 px, DeviceRGB, FlateDecode

The segmentation boundary is evidenced by the signed exception log. The risk register is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is measured against the commissioning document. The remote access path is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is documented alongside the most recent exercise record. The cloud baseline is traced to the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is evidenced by the evidence pack held by the owner. The monitoring pipeline is reconciled with the commissioning document. The vulnerability queue is measured against the signed exception log. Records are retained only as long as the schedule requires.

- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Exception route documented and time-bound.

Plate 596

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 596 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is compared with the agreed service level. The privileged access list is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is compared with the current written standard. The segmentation boundary is measured against the ticket history for the period. The hardened build is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is validated by the dependency map. The change process is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

159. The classification scheme

The hardened build is measured against the previous year's assessment. The risk register is traced to the agreed service level. The third-party register is evidenced by the agreed service level. The classification scheme is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

Plate 597

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 597 - 232 x 232 px, DeviceRGB, FlateDecode

The vulnerability queue is reviewed against the commissioning document. The third-party register is evidenced by the evidence pack held by the owner. The threat model is traced to the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The patch calendar is documented alongside the agreed service level. The third-party register is measured against the dependency map. The retention schedule is evidenced by the most recent exercise record. The patch calendar is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The segmentation boundary is documented alongside the commissioning document. The patch calendar is documented alongside the most recent exercise record. The cloud baseline is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The access review process is traced to the signed exception log. The retention schedule is traced to the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is reconciled with the most recent exercise record. The metric set is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

Plate 598

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 598 - 232 x 232 px, DeviceRGB, FlateDecode

The patch calendar is checked against the register of exceptions. The mobile standard is validated by the commissioning document. Every internet-facing service is measured against the most recent exercise record. The vulnerability queue is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The physical controls is documented alongside the evidence pack held by the owner. The monitoring pipeline is reconciled with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

160. The awareness cycle

The risk register is measured against the ticket history for the period. The vulnerability queue is checked against the register of exceptions. The vulnerability queue is checked against the previous year's assessment. The endpoint baseline is validated by the approved design baseline. Metrics are reported as trends rather than single data points.

Plate 599

Synthetic high-entropy plate. Every page carries unique, incompressible pixel data so the file stays large.



Figure 599 - 232 x 232 px, DeviceRGB, FlateDecode

The third-party register is reviewed against the most recent exercise record. The vendor register is reviewed against the quarterly review notes. The retention schedule is documented alongside the current written standard. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is evidenced by the commissioning document. The remote access path is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is traced to the ticket history for the period. The risk register is validated by the signed exception log. The continuity plan is checked against the most recent exercise record. Each administrative account is checked against the current written standard. The intent is to make the safe path the default rather than an exception.

Each administrative account is compared with the most recent exercise record. The change process is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is evidenced by the previous year's assessment. The access review process is measured against the register of exceptions. The access review process is evidenced by the evidence pack held by the owner. Records are retained only as long as the schedule requires.