STRESS TEST DOCUMENT

Asset Inventory Standard

Benchmark document 22 pages

CYBR-STRESS-020

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.

The threat model is measured against the dependency map. The access review process is documented alongside the previous year's assessment. The physical controls is reconciled with the most recent exercise record. The backup rotation is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

Every internet-facing service is checked against the most recent exercise record. The endpoint baseline is evidenced by the signed exception log. The privileged access list is evidenced by the quarterly review notes. The backup rotation is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

The physical controls is validated by the evidence pack held by the owner. The change process is compared with the commissioning document. The physical controls is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is compared with the commissioning document. The endpoint baseline is reconciled with the signed exception log. The remote access path is measured against the most recent exercise record. The recovery test is measured against the approved design baseline. The control is tested at least once every twelve months.

The privileged access list is validated by the agreed service level. Each administrative account is measured against the approved design baseline. The identity lifecycle is compared with the current written standard. The cloud baseline is compared with the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is validated by the commissioning document. The remote access path is reconciled with the previous year's assessment. The vendor register is reconciled with the quarterly review notes. The backup rotation is compared with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The risk register is compared with the agreed service level. The vendor register is documented alongside the ticket history for the period. The third-party register is evidenced by the dependency map. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is checked against the most recent exercise record. The mobile standard is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is evidenced by the ticket history for the period. The risk register is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The access review process is reviewed against the ticket history for the period. The continuity plan is reconciled with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The change process is reconciled with the evidence pack held by the owner. The patch calendar is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is traced to the current written standard. The monitoring pipeline is reconciled with the evidence pack held by the owner. The access review process is evidenced by the commissioning document. Evidence is kept for audit, insurance and regulator requests.

1. The access review process

The access review process is traced to the evidence pack held by the owner. The vendor register is validated by the most recent exercise record. The continuity plan is evidenced by the most recent exercise record. The endpoint baseline is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The recovery test is reviewed against the previous year's assessment. The encryption standard is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is reconciled with the register of exceptions. The threat model is reconciled with the previous year's assessment. The vendor register is evidenced by the current written standard. The third-party register is checked against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

2. The patch calendar

3. The hardened build

The hardened build is measured against the approved design baseline. The vulnerability queue is reviewed against the ticket history for the period. Each administrative account is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is compared with the quarterly review notes. The threat model is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.

The privileged access list is documented alongside the ticket history for the period. The backup rotation is reviewed against the current written standard. The email authentication record is compared with the most recent exercise record. The vulnerability queue is documented alongside the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is traced to the dependency map. The classification scheme is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The email authentication record is evidenced by the quarterly review notes. The continuity plan is measured against the quarterly review notes. The patch calendar is checked against the evidence pack held by the owner. The privileged access list is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is reviewed against the quarterly review notes. The metric set is measured against the evidence pack held by the owner. The hardened build is measured against the signed exception log. The segmentation boundary is reviewed against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

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

The identity lifecycle is documented alongside the signed exception log. The mobile standard is traced to the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is traced to the approved design baseline. Each administrative account is measured against the evidence pack held by the owner. The remote access path is evidenced by the approved design baseline. The classification scheme is checked against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The metric set is measured against the current written standard. The continuity plan is reconciled with the register of exceptions. Every internet-facing service is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The mobile standard is evidenced by the approved design baseline. The risk register is validated by the agreed service level. The segmentation boundary is evidenced by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The asset register is validated by the agreed service level. The awareness cycle is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The risk register is traced to the dependency map. The remote access path is reconciled with the register of exceptions. The backup rotation is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is measured against the dependency map. The segmentation boundary is reviewed against the ticket history for the period. The backup rotation is checked against the ticket history for the period. The awareness cycle is documented alongside the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

4. The segmentation boundary

The privileged access list is documented alongside the evidence pack held by the owner. The hardened build is validated by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is reviewed against the agreed service level. The access review process is documented alongside the register of exceptions. The risk register is checked against the most recent exercise record. The cloud baseline is validated by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The physical controls is measured against the approved design baseline. The email authentication record is compared with the quarterly review notes. Testing covers the failure case, not only the happy path.

The backup rotation is reconciled with the ticket history for the period. Each administrative account is compared with the current written standard. The encryption standard is reviewed against the evidence pack held by the owner. The asset register is checked against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The change process is traced to the quarterly review notes. The remote access path is reviewed against the commissioning document. The access review process is documented alongside the previous year's assessment. Any deviation requires written approval and an expiry date.

The vendor register is compared with the quarterly review notes. The endpoint baseline is compared with the evidence pack held by the owner. Each administrative account is validated by the quarterly review notes. Every internet-facing service is documented alongside the dependency map. The control is tested at least once every twelve months.

The classification scheme is documented alongside the ticket history for the period. The hardened build is validated by the signed exception log. The backup rotation is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

Every internet-facing service is compared with the approved design baseline. The email authentication record is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.

The metric set is checked against the approved design baseline. The mobile standard is reconciled with the ticket history for the period. Every internet-facing service is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.

The email authentication record is compared with the commissioning document. The metric set is compared with the approved design baseline. The recovery test is checked against the current written standard. The continuity plan is measured against the register of exceptions. The control is tested at least once every twelve months.

The encryption standard is traced to the approved design baseline. The classification scheme is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is documented alongside the signed exception log. The mobile standard is validated by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is checked against the most recent exercise record. The endpoint baseline is reconciled with the quarterly review notes. The risk register is reconciled with the approved design baseline. The identity lifecycle is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The remote access path is evidenced by the evidence pack held by the owner. The retention schedule is documented alongside the evidence pack held by the owner. The risk register is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is checked against the previous year's assessment. The mobile standard is evidenced by the register of exceptions. The endpoint baseline is measured against the agreed service level. The access review process is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The email authentication record is validated by the agreed service level. The vendor register is documented alongside the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The physical controls is documented alongside the approved design baseline. The privileged access list is traced to the current written standard. The recovery test is evidenced by the commissioning document. The risk register is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is reviewed against the dependency map. The change process is checked against the most recent exercise record. The threat model is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is validated by the current written standard. The segmentation boundary is reconciled with the register of exceptions. The retention schedule is documented alongside the quarterly review notes. The third-party register is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is evidenced by the most recent exercise record. The encryption standard is evidenced by the previous year's assessment. The threat model is compared with the evidence pack held by the owner. 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 remote access path is reviewed against the evidence pack held by the owner. The recovery test is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The email authentication record is compared with the signed exception log. The vulnerability queue is evidenced by the evidence pack held by the owner. The vulnerability queue is reviewed against the ticket history for the period. The recovery test is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The metric set is compared with the evidence pack held by the owner. The vendor register is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is compared with the ticket history for the period. The classification scheme is reconciled with the current written standard. The asset register is validated by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

5. The mobile standard

The asset register is measured against the agreed service level. The privileged access list is validated by the signed exception log. The vulnerability queue is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is evidenced by the approved design baseline. Every internet-facing service is traced to the dependency map. The retention schedule is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The patch calendar is compared with the register of exceptions. The vendor register is reviewed against the evidence pack held by the owner. The endpoint baseline is checked against the agreed service level. 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 email authentication record is reviewed against the agreed service level. The recovery test is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

The vulnerability queue is checked against the quarterly review notes. The change process is traced to the dependency map. The retention schedule is documented alongside the most recent exercise record. The vulnerability queue is reconciled with the register of exceptions. Testing covers the failure case, not only the happy path.

The hardened build is reconciled with the ticket history for the period. The remote access path is reviewed against the most recent exercise record. The mobile standard is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is checked against the register of exceptions. The access review process is evidenced by the quarterly review notes. The metric set is validated by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

6. The endpoint baseline

The remote access path is reviewed against the quarterly review notes. The privileged access list is compared with the dependency map. The cloud baseline is evidenced by the dependency map. The asset register is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is measured against the approved design baseline. The endpoint baseline is traced to the quarterly review notes. The vendor register is validated by the previous year's assessment. The control is tested at least once every twelve months.

The asset register is checked against the agreed service level. The awareness cycle is reviewed against the quarterly review notes. The third-party register is compared with the signed exception log. The third-party register is checked against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The asset register is documented alongside the dependency map. The physical controls is documented alongside the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The metric set is checked against the ticket history for the period. The recovery test is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The third-party register is compared with the quarterly review notes. The hardened build is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

The physical controls is documented alongside the quarterly review notes. The cloud baseline is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

The remote access path is traced to the register of exceptions. The classification scheme is reconciled with the quarterly review notes. The email authentication record is validated by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The change process is reconciled with the signed exception log. The access review process is checked against the approved design baseline. The risk register is documented alongside the register of exceptions. The continuity plan is measured against the current written standard. The procedure is written so a new starter can follow it without supervision.

The mobile standard is checked against the approved design baseline. The vulnerability queue is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is compared with the most recent exercise record. The patch calendar is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The third-party register is validated by the most recent exercise record. The third-party register is evidenced by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is reviewed against the signed exception log. The change process is reviewed against the approved design baseline. Each administrative account is evidenced by the quarterly review notes. The risk register is documented alongside the agreed service level. Testing covers the failure case, not only the happy path.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

7. The segmentation boundary

The identity lifecycle is traced to the approved design baseline. The awareness cycle is validated by the signed exception log. The physical controls is reconciled with the register of exceptions. The monitoring pipeline is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is measured against the previous year's assessment. The mobile standard is measured against the signed exception log. The vulnerability queue is compared with the evidence pack held by the owner. The vulnerability queue is checked against the quarterly review notes. Third parties must demonstrate the control before access is granted.

- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.

The vendor register is validated by the commissioning document. The monitoring pipeline is checked against the approved design baseline. The monitoring pipeline is compared with the most recent exercise record. The endpoint baseline is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is documented alongside the most recent exercise record. The risk register is checked against the commissioning document. The classification scheme is documented alongside the register of exceptions. The cloud baseline is measured against the quarterly review notes. Records are retained only as long as the schedule requires.

The vulnerability queue is measured against the agreed service level. The email authentication record is traced to the agreed service level. The classification scheme is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The encryption standard is reconciled with the most recent exercise record. The retention schedule is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The asset register is reconciled with the ticket history for the period. The endpoint baseline is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The identity lifecycle is compared with the commissioning document. The threat model is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

The access review process is compared with the signed exception log. The encryption standard is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the register of exceptions. The endpoint baseline is measured against the commissioning document. The third-party register is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The threat model is measured against the dependency map. The recovery test is reviewed against the register of exceptions. The monitoring pipeline is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The change process is compared with the most recent exercise record. The risk register is validated by the most recent exercise record. The mobile standard is compared with the signed exception log. The awareness cycle is reconciled with the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The metric set is checked against the dependency map. The vulnerability queue is documented alongside the quarterly review notes. Any deviation requires written approval and an expiry date.

The change process is evidenced by the most recent exercise record. Each administrative account is traced to the most recent exercise record. The hardened build is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

The metric set is compared with the approved design baseline. The threat model is evidenced by the agreed service level. Each administrative account is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The encryption standard is evidenced by the previous year's assessment. The hardened build 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 vendor register is evidenced by the evidence pack held by the owner. The remote access path is checked against the register of exceptions. The mobile standard is reviewed against the quarterly review notes. The patch calendar is checked against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

8. The third-party register

The recovery test is reviewed against the quarterly review notes. The monitoring pipeline is evidenced by the agreed service level. The recovery test 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 email authentication record is reconciled with the ticket history for the period. The hardened build is traced to the ticket history for the period. The vendor register is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is reconciled with the evidence pack held by the owner. The continuity plan is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

The remote access path is reconciled with the evidence pack held by the owner. The patch calendar is reviewed against the previous year's assessment. Every internet-facing service 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 segmentation boundary is evidenced by the agreed service level. The patch calendar is evidenced by the evidence pack held by the owner. The encryption standard is documented alongside the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

9. The continuity plan

The threat model is reviewed against the commissioning document. The awareness cycle is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The continuity plan is compared with the approved design baseline. The remote access path is compared with the dependency map. The cloud baseline is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

The email authentication record is reviewed against the current written standard. The monitoring pipeline is compared with the previous year's assessment. The physical controls is validated by the current written standard. Metrics are reported as trends rather than single data points.

The vendor register is evidenced by the quarterly review notes. The third-party register is reconciled with the most recent exercise record. The segmentation boundary is validated by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

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

The retention schedule is reconciled with the agreed service level. The metric set is documented alongside the commissioning document. The classification scheme is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is reviewed against the approved design baseline. The email authentication record is traced to the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is reconciled with the evidence pack held by the owner. The mobile standard is documented alongside the agreed service level. The asset register is compared with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is measured against the approved design baseline. The retention schedule is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The metric set is documented alongside the most recent exercise record. The threat model 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 identity lifecycle is compared with the evidence pack held by the owner. The cloud baseline is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is reviewed against the previous year's assessment. The awareness cycle is measured against the most recent exercise record. The segmentation boundary is reviewed against the most recent exercise record. The continuity plan is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The vendor register is documented alongside the current written standard. The cloud baseline is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The asset register is evidenced by the current written standard. The threat model is compared with the ticket history for the period. Every internet-facing service is evidenced by the register of exceptions. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reviewed against the signed exception log. The retention schedule is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The access review process is measured against the quarterly review notes. The retention schedule is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is checked against the register of exceptions. The backup rotation is reviewed against the approved design baseline. The classification scheme is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Test result attached to the record.

The third-party register is validated by the agreed service level. The hardened build is measured against the previous year's assessment. The monitoring pipeline is evidenced by the signed exception log. The threat model is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

The third-party register is validated by the commissioning document. The hardened build is checked against the agreed service level. The intent is to make the safe path the default rather than an exception.

The third-party register is measured against the previous year's assessment. The classification scheme is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is traced to the approved design baseline. The encryption standard is reconciled with the register of exceptions. The control is tested at least once every twelve months.

The encryption standard is reconciled with the most recent exercise record. The email authentication record is reconciled with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The vendor register is validated by the most recent exercise record. The retention schedule is reconciled with the previous year's assessment. The privileged access list is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The privileged access list is evidenced by the commissioning document. The mobile standard is compared with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The mobile standard is measured against the quarterly review notes. The backup rotation is documented alongside the most recent exercise record. The vendor register is compared with the ticket history for the period. The threat model is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The threat model is documented alongside the most recent exercise record. The vendor register is validated by the ticket history for the period. Any deviation requires written approval and an expiry date.

The segmentation boundary is documented alongside the most recent exercise record. The threat model is compared with the previous year's assessment. The recovery test is traced to the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is reviewed against the signed exception log. The continuity plan is evidenced by the agreed service level. The control is tested at least once every twelve months.

The metric set is compared with the ticket history for the period. The risk register is evidenced by the agreed service level. The endpoint baseline is compared with the evidence pack held by the owner. The backup rotation is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is checked against the most recent exercise record. The backup rotation is evidenced by the dependency map. The vulnerability queue is evidenced by the ticket history for the period. The risk register is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The asset register is documented alongside the register of exceptions. The monitoring pipeline is reconciled with the evidence pack held by the owner. The retention schedule is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

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

The continuity plan is reconciled with the agreed service level. The monitoring pipeline is measured against the ticket history for the period. The email authentication record is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

Each administrative account is validated by the quarterly review notes. The encryption standard is documented alongside the ticket history for the period. The continuity plan is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

- Test result attached to the record.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.

The physical controls is compared with the commissioning document. The recovery test is evidenced by the signed exception log. The retention schedule is traced to the approved design baseline. The monitoring pipeline is checked against the quarterly review notes. Any deviation requires written approval and an expiry date.

10. The retention schedule

The hardened build is documented alongside the evidence pack held by the owner. Each administrative account is traced to the evidence pack held by the owner. The change process is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Exception route documented and time-bound.

The physical controls is validated by the evidence pack held by the owner. The asset register is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the dependency map. The asset register is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reviewed against the agreed service level. The awareness cycle is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is documented alongside the most recent exercise record. The risk register is reviewed against the signed exception log. 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 reviewed against the register of exceptions. The segmentation boundary is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The hardened build is validated by the evidence pack held by the owner. The risk register is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The email authentication record is reviewed against the current written standard. The physical controls is compared with the agreed service level. The hardened build is measured against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is reconciled with the evidence pack held by the owner. The retention schedule is compared with 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 cloud baseline is reviewed against the quarterly review notes. Each administrative account is validated by the evidence pack held by the owner. The mobile standard is compared with the dependency map. Metrics are reported as trends rather than single data points.

The physical controls is evidenced by the dependency map. The continuity plan is checked against the approved design baseline. The continuity plan is compared with the quarterly review notes. The segmentation boundary is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The recovery test is documented alongside the ticket history for the period. Every internet-facing service is documented alongside the quarterly review notes. Records are retained only as long as the schedule requires.

The endpoint baseline is evidenced by the current written standard. The risk 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 compared with the quarterly review notes. The recovery test is measured against the evidence pack held by the owner. Every internet-facing service is documented alongside the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is validated by the previous year's assessment. The email authentication record is measured against the commissioning document. The remote access path is documented alongside the most recent exercise record. Third parties must demonstrate the control before access is granted.

The backup rotation is documented alongside the agreed service level. The encryption standard is validated by the commissioning document. The monitoring pipeline is measured against the ticket history for the period. The risk register is evidenced by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

11. The identity lifecycle

The third-party register is compared with the evidence pack held by the owner. The privileged access list is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The monitoring pipeline is evidenced by the previous year's assessment. The retention schedule is checked against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is documented alongside the signed exception log. The risk register is evidenced by the previous year's assessment. The segmentation boundary is reviewed against the signed exception log. The classification scheme is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

12. The email authentication record

The remote access path is traced to the commissioning document. The identity lifecycle is traced to the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the most recent exercise record. The mobile standard is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The risk register is reviewed against the signed exception log. The retention schedule is validated by the evidence pack held by the owner. The email authentication record is documented alongside the dependency map. Records are retained only as long as the schedule requires.

The privileged access list is reviewed against the signed exception log. Each administrative account is checked against the current written standard. The vendor register is compared with the approved design baseline. The retention schedule is traced to the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reconciled with the dependency map. The third-party register is evidenced by the dependency map. The metric set is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is validated by the most recent exercise record. The monitoring pipeline is validated by the register of exceptions. The control is tested at least once every twelve months.

The segmentation boundary is checked against the ticket history for the period. The metric set is validated by the previous year's assessment. The hardened build is documented alongside the register of exceptions. The risk register is validated by the current written standard. Metrics are reported as trends rather than single data points.

The risk register is measured against the agreed service level. Each administrative account is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is reviewed against the approved design baseline. The patch calendar is measured against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is validated by the register of exceptions. The privileged access list is evidenced by the evidence pack held by the owner. The continuity plan is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The identity lifecycle is traced to the signed exception log. The identity lifecycle is checked against the register of exceptions. The asset register is reviewed against the register of exceptions. The third-party register is evidenced by the signed exception log. The procedure is written so a new starter can follow it without supervision.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Exception route documented and time-bound.

The encryption standard is validated by the previous year's assessment. The continuity plan is reconciled with the evidence pack held by the owner. The third-party register is reconciled with the quarterly review notes. The classification scheme is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

13. The retention schedule

The patch calendar is compared with the register of exceptions. The privileged access list 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 vendor register is validated by the dependency map. The asset register is evidenced by the register of exceptions. The privileged access list is measured against the most recent exercise record. The control is tested at least once every twelve months.

The encryption standard is evidenced by the ticket history for the period. The classification scheme is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The monitoring pipeline is reviewed against the dependency map. The identity lifecycle is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

The asset register is documented alongside the ticket history for the period. The hardened build is measured against the current written standard. The physical controls is documented alongside the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The metric set is validated by the previous year's assessment. The endpoint baseline is measured against the most recent exercise record. The email authentication record is reviewed against the most recent exercise record. The remote access path is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

14. The segmentation boundary

The access review process is evidenced by the agreed service level. The awareness cycle is reconciled with the most recent exercise record. The email authentication record is measured against the quarterly review notes. The identity lifecycle is documented alongside the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is reconciled with the agreed service level. The monitoring pipeline is measured against the evidence pack held by the owner. The identity lifecycle is reconciled with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is reviewed against the quarterly review notes. The mobile standard is evidenced by the commissioning document. The risk register is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is checked against the evidence pack held by the owner. The classification scheme is compared with the register of exceptions. The monitoring pipeline is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is documented alongside the ticket history for the period. The metric set is compared with the dependency map. The remote access path is traced to the signed exception log. The recovery test is reviewed against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the commissioning document. The remote access path is reconciled with the signed exception log. The privileged access list is checked against the previous year's assessment. Every internet-facing service is reviewed against the register of exceptions. The control is tested at least once every twelve months.

The mobile standard is measured against the approved design baseline. The vulnerability queue is compared with the approved design baseline. The retention schedule is measured against the signed exception log. Each administrative account is compared with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The remote access path is reviewed against the register of exceptions. The retention schedule is validated by the current written standard. The endpoint baseline is traced to the ticket history for the period. The retention schedule is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is reviewed against the current written standard. The risk register is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is measured against the most recent exercise record. The retention schedule is reviewed against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is measured against the register of exceptions. The retention schedule is reviewed against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The physical controls is reviewed against the agreed service level. The mobile standard is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is validated by the dependency map. The hardened build is reconciled with the current written standard. The identity lifecycle is measured against the dependency map. The mobile standard is compared with the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

15. The continuity plan

The recovery test is evidenced by the agreed service level. Every internet-facing service is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

- Review date scheduled and visible.
- Test result attached to the record.
- Notification list confirmed before execution.
- Exception route documented and time-bound.

The privileged access list is compared with the ticket history for the period. The threat model is reconciled with the signed exception log. The risk register is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is validated by the evidence pack held by the owner. The vulnerability queue is documented alongside the previous year's assessment. The remote access path is reviewed against the agreed service level. The metric set is checked against the commissioning document. Testing covers the failure case, not only the happy path.

The third-party register is documented alongside the commissioning document. The third-party register is evidenced by the current written standard. The patch calendar is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the previous year's assessment. The segmentation boundary is reconciled with the evidence pack held by the owner. The remote access path is validated by the agreed service level. Testing covers the failure case, not only the happy path.

The risk register is reconciled with the previous year's assessment. The awareness cycle is evidenced by the ticket history for the period. The encryption standard is measured against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is compared with the previous year's assessment. The email authentication record is validated by the signed exception log. The encryption standard is checked against the register of exceptions. Testing covers the failure case, not only the happy path.

Each administrative account is documented alongside the approved design baseline. The classification scheme is reviewed against the agreed service level. The hardened build is evidenced by the agreed service level. The recovery test is documented alongside the current written standard. The measure applies equally to staff, contractors and managed service providers.

The risk register is reviewed against the evidence pack held by the owner. The endpoint baseline is validated by the current written standard. The email authentication record is reviewed against the approved design baseline. Third parties must demonstrate the control before access is granted.

The threat model is compared with the current written standard. The vendor register is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is measured against the ticket history for the period. The asset register is traced to the approved design baseline. The vendor register is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is checked against the ticket history for the period. The classification scheme is compared with the signed exception log. The segmentation boundary is validated by the ticket history for the period. The control is tested at least once every twelve months.

The identity lifecycle is measured against the approved design baseline. Every internet-facing service is evidenced by the commissioning document. 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.

The recovery test is compared with the commissioning document. The email authentication record is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.

The asset register is traced to the current written standard. The cloud baseline is reconciled with the agreed service level. Any deviation requires written approval and an expiry date.

The cloud baseline is documented alongside the quarterly review notes. The change process is reconciled with the current written standard. The identity lifecycle is reconciled with the evidence pack held by the owner. The metric set is evidenced by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is checked against the approved design baseline. The mobile standard is checked against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is checked against the approved design baseline. The physical controls is checked against the quarterly review notes. The risk register is documented alongside the agreed service level. The asset register is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

17. The retention schedule

The retention schedule is reconciled with the current written standard. The encryption standard is reconciled with the signed exception log. Any deviation requires written approval and an expiry date.