Privileged Access Programme

Procedure 21 pages

CYBR-STRESS-051

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 validated by the register of exceptions. The third-party register is reconciled with the approved design baseline. The patch calendar is documented alongside the previous year's assessment. The email authentication record is traced to the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

1. The patch calendar

The privileged access list is traced to the dependency map. The physical controls is evidenced by the signed exception log. The identity lifecycle is measured against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is reviewed against the previous year's assessment. The vendor register is compared with the signed exception log. The continuity plan is reconciled with the register of exceptions. The asset register is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

2. The vendor register

The mobile standard is validated by the most recent exercise record. The metric set is evidenced by the previous year's assessment. The change process is evidenced by the most recent exercise record. The vulnerability queue is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is checked against the most recent exercise record. The privileged access list is validated by the register of exceptions. The change process is reviewed against the evidence pack held by the owner. The awareness cycle is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is reviewed against the previous year's assessment. The third-party register is measured against the signed exception log. The email authentication record is evidenced by the signed exception log. The retention schedule is reviewed against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

3. Every internet-facing service

The email authentication record is validated by the current written standard. The retention schedule is checked against the agreed service level. The privileged access list is evidenced by the quarterly review notes. The monitoring pipeline is validated by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Test result attached to the record.

The endpoint baseline is evidenced by the most recent exercise record. The endpoint baseline is measured against the most recent exercise record. The endpoint baseline is evidenced by the evidence pack held by the owner. The backup rotation is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

4. The segmentation boundary

The backup rotation is reviewed against the ticket history for the period. The email authentication record is reviewed against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

5. The third-party register

The cloud baseline is evidenced by the register of exceptions. The hardened build is documented alongside the commissioning document. The metric set 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 traced to the current written standard. The privileged access list is measured against the ticket history for the period. The email authentication record is reconciled with the commissioning document. The encryption standard is checked against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The physical controls is compared with the agreed service level. The retention schedule is reconciled with the register of exceptions. Any deviation requires written approval and an expiry date.

The change process is reconciled with the approved design baseline. The awareness cycle is reviewed against the dependency map. The encryption standard 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. The awareness cycle is reconciled with the dependency map. The encryption standard is checked against the register of exceptions. The third-party register is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is evidenced by the approved design baseline. The hardened build is reconciled with the quarterly review notes. Any deviation requires written approval and an expiry date.

The privileged access list is reconciled with the register of exceptions. The threat model is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

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

The encryption standard is evidenced by the dependency map. The threat model is reviewed against the approved design baseline. The privileged access list is checked against the previous year's assessment. The vendor register is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The access review process is documented alongside the approved design baseline. The recovery test is documented alongside the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is documented alongside the most recent exercise record. The cloud baseline is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is measured against the ticket history for the period. Each administrative account is measured against the previous year's assessment. Each administrative account is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is compared with the commissioning document. The classification scheme is validated by the register of exceptions. The access review process is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The encryption standard is measured against the commissioning document. The remote access path is checked against the ticket history for the period. The recovery test is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

6. The identity lifecycle

The monitoring pipeline is validated by the quarterly review notes. The retention schedule is validated by the dependency map. The physical controls is compared with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is compared with the approved design baseline. Every internet-facing service is documented alongside the commissioning document. The identity lifecycle is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

The monitoring pipeline is compared with the current written standard. The hardened build is measured against the ticket history for the period. The third-party register is checked against the dependency map. The vulnerability queue is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The change process is traced to the current written standard. The physical controls is measured against the quarterly review notes. The monitoring pipeline is compared with the previous year's assessment. The risk register is documented alongside the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is reconciled with the quarterly review notes. The metric set is checked against the quarterly review notes. The risk register is checked against the most recent exercise record. The email authentication record is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

The threat model is traced to the quarterly review notes. The monitoring pipeline is measured against the signed exception log. The third-party register is reviewed against the dependency map. The vendor register is checked against the most recent exercise record. The control is tested at least once every twelve months.

The cloud baseline is compared with the ticket history for the period. The segmentation boundary is documented alongside the commissioning document. The identity lifecycle is validated by the approved design baseline. The retention schedule is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is measured against the agreed service level. The awareness cycle is compared with the current written standard. Each administrative account is traced to the signed exception log. Metrics are reported as trends rather than single data points.

Every internet-facing service is reviewed against the approved design baseline. The third-party register is traced to the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is reconciled with the dependency map. The continuity plan is reconciled with the evidence pack held by the owner. The email authentication record is compared with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is evidenced by the agreed service level. The hardened build is validated by the commissioning document. The encryption standard is checked against the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is reviewed against the evidence pack held by the owner. The encryption standard is validated by the ticket history for the period. The email authentication record is evidenced by the most recent exercise record. The endpoint baseline is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The recovery test is documented alongside the approved design baseline. The continuity plan is compared with the approved design baseline. The third-party register is reviewed against the quarterly review notes. The threat model is evidenced by the most recent exercise record. The control is tested at least once every twelve months.

The privileged access list is traced to the quarterly review notes. The metric set is compared with the approved design baseline. The threat model is traced to the ticket history for the period. Any deviation requires written approval and an expiry date.

The remote access path is traced to the approved design baseline. The vulnerability queue is compared with the most recent exercise record. The remote access path is reconciled with the evidence pack held by the owner. The asset register is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is reviewed against the signed exception log. The access review process is traced to the previous year's assessment. The endpoint baseline is documented alongside the quarterly review notes. The email authentication record is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The change process is checked against the dependency map. The endpoint baseline is traced to the previous year's assessment. The threat model is reviewed against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is checked against the agreed service level. The cloud baseline is compared with the approved design baseline. Records are retained only as long as the schedule requires.

The endpoint baseline is measured against the quarterly review notes. The third-party register is validated by the register of exceptions. The remote access path is documented alongside the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The metric set is reviewed against the agreed service level. The physical controls is validated by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The physical controls is measured against the previous year's assessment. The change process is validated by the ticket history for the period. The privileged access list is validated by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

7. The patch calendar

The endpoint baseline is reconciled with the most recent exercise record. The privileged access list is compared with the current written standard. Records are retained only as long as the schedule requires.

The vulnerability queue is documented alongside the most recent exercise record. The threat model is documented alongside the previous year's assessment. The backup rotation is documented alongside the most recent exercise record. The backup rotation is reviewed against the approved design baseline. Third parties must demonstrate the control before access is granted.

The vulnerability queue is measured against the agreed service level. The mobile standard is reviewed against the agreed service level. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reconciled with the most recent exercise record. Each administrative account is reconciled with the dependency map. The identity lifecycle is checked against the current written standard. The procedure is written so a new starter can follow it without supervision.

The email authentication record is validated by the register of exceptions. The endpoint baseline is reconciled with the most recent exercise record. The monitoring pipeline is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The classification scheme is evidenced by the agreed service level. The email authentication record is documented alongside the agreed service level. Each administrative account is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The cloud baseline is compared with the signed exception log. The risk register is reviewed against the most recent exercise record. The asset register is evidenced by the signed exception log. The encryption standard is validated by the dependency map. Testing covers the failure case, not only the happy path.

The backup rotation is evidenced by the previous year's assessment. The remote access path is documented alongside the commissioning document. The patch calendar is documented alongside the ticket history for the period. The change process is traced to the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The metric set is validated by the signed exception log. The encryption standard is checked against the register of exceptions. The risk register is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

The classification scheme is documented alongside the quarterly review notes. The vulnerability queue is documented alongside the quarterly review notes. The hardened build is documented alongside the dependency map. The identity lifecycle is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is compared with the previous year's assessment. Each administrative account is traced to the current written standard. The backup rotation is reviewed against the register of exceptions. The continuity plan is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is documented alongside the agreed service level. The risk register is documented alongside the ticket history for the period. The privileged access list is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

The vendor register is validated by the agreed service level. The continuity plan is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reviewed against the approved design baseline. The vulnerability queue is compared with the approved design baseline. Every internet-facing service is measured against the approved design baseline. The backup rotation is traced to the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.

The endpoint baseline is documented alongside the current written standard. The threat model is documented alongside the previous year's assessment. The awareness cycle is traced to the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The change process is traced to the quarterly review notes. Each administrative account is measured against the approved design baseline. The vendor register is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is checked against the commissioning document. The encryption standard is reviewed against the ticket history for the period. The control is tested at least once every twelve months.

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

The patch calendar is measured against the ticket history for the period. The backup rotation is validated by the ticket history for the period. The hardened build is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The continuity plan is compared with the commissioning document. The recovery test is reviewed against the evidence pack held by the owner. The third-party register is measured against the most recent exercise record. The awareness cycle is reviewed against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

- Test result attached to the record.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.

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

The hardened build is documented alongside the commissioning document. The backup rotation is reconciled with the previous year's assessment. The access review process is checked against the approved design baseline. The access review process is checked against the register of exceptions. Metrics are reported as trends rather than single data points.

The vendor register is documented alongside the previous year's assessment. The awareness cycle is traced to the signed exception log. The physical controls is compared with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is evidenced by the signed exception log. The mobile standard is traced to the previous year's assessment. Each administrative account is compared with the current written standard. The segmentation boundary is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is checked against the most recent exercise record. Every internet-facing service is reconciled with the signed exception log. Third parties must demonstrate the control before access is granted.

The change process is compared with the previous year's assessment. Every internet-facing service is reconciled with the dependency map. The threat model is validated by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is documented alongside the most recent exercise record. The identity lifecycle is reconciled with the register of exceptions. The recovery test is reviewed against the signed exception log. The classification scheme is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is checked against the signed exception log. The vulnerability queue is reconciled with the current written standard. The recovery test is evidenced by the ticket history for the period. The access review process is measured against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The change process is reviewed against the quarterly review notes. The awareness cycle is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The threat model is validated by the evidence pack held by the owner. The identity lifecycle is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is documented alongside the register of exceptions. The threat model is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

The segmentation boundary is evidenced by the dependency map. The retention schedule is validated by the register of exceptions. The remote access path is traced to the quarterly review notes. 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.

8. The physical controls

Every internet-facing service is compared with the commissioning document. The monitoring pipeline is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The recovery test is measured against the previous year's assessment. The monitoring pipeline is evidenced by the current written standard. The patch calendar is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The continuity plan is traced to the register of exceptions. The physical controls is compared with the ticket history for the period. The identity lifecycle is reviewed against the previous year's assessment. The patch calendar is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is reconciled with the ticket history for the period. The metric set is reviewed against the previous year's assessment. The backup rotation is measured against the agreed service level. The patch calendar is reviewed against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is reviewed against the quarterly review notes. The recovery test is documented alongside the evidence pack held by the owner. The endpoint baseline is measured against the dependency map. The cloud baseline is checked against 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 measured against the most recent exercise record. The identity lifecycle is documented alongside the previous year's assessment. The monitoring pipeline is reconciled with the commissioning document. The monitoring pipeline is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

- Test result attached to the record.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

The segmentation boundary is evidenced by the signed exception log. The change process is traced to the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The hardened build is validated by the previous year's assessment. The segmentation boundary is reviewed against the agreed service level. The continuity plan is measured against the signed exception log. The hardened build is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is reviewed against the signed exception log. The threat model is compared with the approved design baseline. The backup rotation is reconciled with the dependency map. The access review process is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is validated by the quarterly review notes. The hardened build is evidenced by the quarterly review notes. The physical controls is validated by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is evidenced by the approved design baseline. The cloud baseline is reviewed against the dependency map. The endpoint baseline is documented alongside the signed exception log. Third parties must demonstrate the control before access is granted.

The metric set is checked against the previous year's assessment. Each administrative account is evidenced by the signed exception log. Each administrative account is checked against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The classification scheme is reviewed against the register of exceptions. The metric set is evidenced by the evidence pack held by the owner. The cloud baseline is reconciled with the commissioning document. The classification scheme is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The remote access path is reconciled with the previous year's assessment. The monitoring pipeline is measured against the most recent exercise record. The patch calendar is checked against the ticket history for the period. The recovery test is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

9. The endpoint baseline

The segmentation boundary is measured against the signed exception log. The hardened build is reconciled with the ticket history for the period. The monitoring pipeline is traced to the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is checked against the approved design baseline. The identity lifecycle is checked against the current written standard. The classification scheme is traced to the approved design baseline. The backup rotation is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the evidence pack held by the owner. The monitoring pipeline is validated by the signed exception log. The physical controls is checked against the register of exceptions. Every internet-facing service is reconciled with the signed exception log. Any deviation requires written approval and an expiry date.

The classification scheme is compared with the dependency map. The recovery test is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

10. The backup rotation

The access review process is compared with the agreed service level. The segmentation boundary is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The risk register is checked against the previous year's assessment. Every internet-facing service is compared with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Test result attached to the record.

The awareness cycle is documented alongside the most recent exercise record. The endpoint baseline is traced to the current written standard. The awareness cycle is measured against the previous year's assessment. The recovery test is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The recovery test is traced to the dependency map. The email authentication record is checked against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is validated by the signed exception log. The third-party register is reviewed against the ticket history for the period. The segmentation boundary is documented alongside the current written standard. The monitoring pipeline is reviewed against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is validated by the register of exceptions. The endpoint baseline is reviewed against the evidence pack held by the owner. The asset register is reconciled with the ticket history for the period. The physical controls is documented alongside the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The backup rotation is measured against the current written standard. The metric set is documented alongside the previous year's assessment. The risk register is measured against the evidence pack held by the owner. The encryption standard is reviewed against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is traced to the approved design baseline. The physical controls is checked against the dependency map. The threat model is reconciled with the dependency map. The monitoring pipeline is traced to the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The threat model is documented alongside the quarterly review notes. The cloud baseline is checked against the register of exceptions. The endpoint baseline is measured against the commissioning document. Third parties must demonstrate the control before access is granted.

The patch calendar is reviewed against the most recent exercise record. The recovery test is measured against the commissioning document. The cloud baseline is documented alongside the dependency map. Where automation is possible, the manual step is retained as a fallback.

The risk register is checked against the register of exceptions. The risk register is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is checked against the previous year's assessment. The metric set is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is compared with the commissioning document. The vendor register is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The remote access path is documented alongside the quarterly review notes. The threat model is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

The privileged access list is compared with the evidence pack held by the owner. The backup rotation 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 identity lifecycle is checked against the previous year's assessment. The risk register is compared with the current written standard. The encryption standard is documented alongside the approved design baseline. The access review process is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The metric set is measured against the register of exceptions. The classification scheme is traced to the most recent exercise record. The threat model is checked against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The metric set is validated by the previous year's assessment. The monitoring pipeline is evidenced by the previous year's assessment. Testing covers the failure case, not only the happy path.

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

The mobile standard is validated by the ticket history for the period. The hardened build is checked against the dependency map. The risk register is compared with the signed exception log. The privileged access list is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The cloud baseline is evidenced by the dependency map. Every internet-facing service is compared with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is reconciled with the agreed service level. Each administrative account is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The physical controls is evidenced by the commissioning document. The metric set is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

11. The metric set

The third-party register is validated by the signed exception log. The hardened build is validated by the current written standard. Any deviation requires written approval and an expiry date.

Each administrative account is reconciled with the ticket history for the period. The endpoint baseline is checked against the commissioning document. The intent is to make the safe path the default rather than an exception.

The classification scheme is compared with the ticket history for the period. The monitoring pipeline is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The access review process is validated by the agreed service level. The endpoint baseline is traced to the commissioning document. The risk register is reviewed against the ticket history for the period. The continuity plan is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The backup rotation is documented alongside the dependency map. The continuity plan is validated by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is evidenced by the register of exceptions. The physical controls is documented alongside the signed exception log. The patch calendar is reconciled with the evidence pack held by the owner. The threat model is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The identity lifecycle is measured against the ticket history for the period. The third-party register is measured against the approved design baseline. Third parties must demonstrate the control before access is granted.

The cloud baseline is reviewed against the register of exceptions. The recovery test is reconciled with the approved design baseline. The asset register is traced to the dependency map. The asset register is measured against the quarterly review notes. The control is tested at least once every twelve months.

The backup rotation is evidenced by the approved design baseline. The mobile standard is reviewed against the previous year's assessment. The backup rotation is checked against the agreed service level. The retention schedule is documented alongside the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The classification scheme is checked against the quarterly review notes. The cloud baseline is traced to the ticket history for the period. The third-party register is traced to the agreed service level. The asset register is validated by the dependency map. Testing covers the failure case, not only the happy path.

The monitoring pipeline is traced to the dependency map. The continuity plan is compared with the most recent exercise record. The privileged access list is reconciled with the most recent exercise record. The email authentication record is traced to the agreed service level. Metrics are reported as trends rather than single data points.

- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.

Each administrative account is checked against the current written standard. The endpoint baseline is evidenced by the current written standard. The asset register is validated by the dependency map. The monitoring pipeline is checked against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is checked against the evidence pack held by the owner. Each administrative account is checked against the previous year's assessment. The encryption standard is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The third-party register is evidenced by the approved design baseline. The retention schedule is checked against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Review date scheduled and visible.

The risk register is checked against the signed exception log. Every internet-facing service is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The endpoint baseline is reconciled with the commissioning document. The patch calendar is reconciled with the dependency map. Each administrative account is reviewed against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is evidenced by the evidence pack held by the owner. The third-party register is reconciled with the agreed service level. The mobile standard is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

The remote access path is reviewed against the commissioning document. The asset register is compared with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is validated by the signed exception log. The classification scheme is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The cloud baseline is reviewed against the dependency map. The backup rotation is measured against the previous year's assessment. The remote access path is validated by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is documented alongside the commissioning document. The threat model is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is validated by the dependency map. Each administrative account is documented alongside the dependency map. The hardened build is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Test result attached to the record.
- Notification list confirmed before execution.

The retention schedule is reviewed against the approved design baseline. The segmentation boundary is reviewed against the current written standard. Each administrative account is reconciled with the commissioning document. The patch calendar is evidenced by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is validated by the signed exception log. The monitoring pipeline is measured against the agreed service level. Records are retained only as long as the schedule requires.

The segmentation boundary is documented alongside the approved design baseline. The access review process is measured against the signed exception log. The threat model is checked against the most recent exercise record. The backup rotation is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

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

The retention schedule is reviewed against the quarterly review notes. The mobile standard is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The access review process is reviewed against the register of exceptions. The patch calendar is reviewed against the signed exception log. The control is tested at least once every twelve months.

The vendor register is traced to the approved design baseline. The continuity plan is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

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

The threat model is validated by the quarterly review notes. The third-party register is reviewed against the agreed service level. The patch calendar is checked against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is checked against the approved design baseline. The endpoint baseline is reviewed against the ticket history for the period. 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 third-party register is documented alongside the evidence pack held by the owner. The physical controls is documented alongside the commissioning document. The monitoring pipeline is validated by the most recent exercise record. The email authentication record is checked against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The physical controls is documented alongside the dependency map. The mobile standard is documented alongside the commissioning document. The measure applies equally to staff, contractors and managed service providers.

- Evidence stored in the shared evidence pack.
- 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 vendor register is reconciled with the approved design baseline. The third-party register is compared with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is documented alongside the quarterly review notes. The segmentation boundary is reconciled with the approved design baseline. The third-party register is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The vendor register is traced to the signed exception log. The vendor register is evidenced by the register of exceptions. The remote access path is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The vendor register is measured against the signed exception log. The change process is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

12. The metric set

The endpoint baseline is evidenced by the register of exceptions. The privileged access list is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The metric set is documented alongside the agreed service level. The metric set is traced to the register of exceptions. The retention schedule is validated by the dependency map. The patch calendar is measured against the register of exceptions. Records are retained only as long as the schedule requires.

The segmentation boundary is documented alongside the current written standard. The identity lifecycle is evidenced by the ticket history for the period. The backup rotation is validated by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is validated by the ticket history for the period. The vulnerability queue is traced to the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is reconciled with the signed exception log. The segmentation boundary is documented alongside the current written standard. The recovery test is reviewed against the most recent exercise record. The cloud baseline is compared with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The backup rotation is validated by the current written standard. The cloud baseline is documented alongside the most recent exercise record. The vulnerability queue is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is reviewed against the quarterly review notes. The vendor register is checked against the previous year's assessment. The identity lifecycle is reconciled with the most recent exercise record. The retention schedule is compared with the register of exceptions. The control is tested at least once every twelve months.

The patch calendar is traced to the register of exceptions. The retention schedule is traced to the signed exception log. The classification scheme is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The email authentication record is validated by the current written standard. The continuity plan is reviewed against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The privileged access list is validated by the signed exception log. The classification scheme is documented alongside the agreed service level. The backup rotation is traced to the commissioning document. The vulnerability queue is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The awareness cycle is evidenced by the signed exception log. The threat model is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is measured against the register of exceptions. The vendor register is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is documented alongside the approved design baseline. The risk register is documented alongside the previous year's assessment. The patch calendar is documented alongside the approved design baseline. The cloud baseline is documented alongside the dependency map. Evidence is kept for audit, insurance and regulator requests.

The remote access path is checked against the current written standard. Every internet-facing service is measured against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is evidenced by the dependency map. The email authentication record is reconciled with the signed exception log. Any deviation requires written approval and an expiry date.

13. The email authentication record

The threat model is compared with the previous year's assessment. The patch calendar is measured against the most recent exercise record. The physical controls is documented alongside the dependency map. Each administrative account is checked against the agreed service level. Testing covers the failure case, not only the happy path.

The third-party register is reviewed against the evidence pack held by the owner. The encryption standard is documented alongside the register of exceptions. The endpoint baseline is evidenced by the current written standard. The threat model is checked against the approved design baseline. The intent is to make the safe path the default rather than an exception.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.

The change process is measured against the signed exception log. The patch calendar is validated by the previous year's assessment. The cloud baseline is compared with the agreed service level. Third parties must demonstrate the control before access is granted.

The physical controls is reconciled with the ticket history for the period. The risk register is documented alongside the evidence pack held by the owner. The recovery test is reconciled with the current written standard. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is validated by the register of exceptions. The cloud baseline is traced to the previous year's assessment. The physical controls is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The metric set is evidenced by the agreed service level. The change process is traced to the agreed service level. The email authentication record is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is reviewed against the ticket history for the period. The patch calendar is validated by the register of exceptions. The patch calendar is evidenced by the agreed service level. The threat model is reconciled with 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 register of exceptions. The encryption standard is traced to the dependency map. Every internet-facing service is measured against the ticket history for the period. Records are retained only as long as the schedule requires.

The backup rotation is compared with the most recent exercise record. The vendor register is traced to the ticket history for the period. The vendor register is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

14. The risk register

The segmentation boundary is documented alongside the dependency map. The vulnerability queue is evidenced by the most recent exercise record. The patch calendar is checked against the evidence pack held by the owner. The mobile standard is documented alongside the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The change process is validated by the dependency map. The mobile standard is compared with the quarterly review notes. The metric set is checked against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The hardened build is compared with the signed exception log. The vulnerability queue is compared with the most recent exercise record. The vulnerability queue is compared with the commissioning document. The encryption standard is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is evidenced by the quarterly review notes. The encryption standard is checked against the agreed service level. The privileged access list is checked against the dependency map. Each administrative account is measured against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The continuity plan is evidenced by the commissioning document. The third-party register is checked against the current written standard. The email authentication record is validated by the agreed service level. The backup rotation is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is evidenced by the previous year's assessment. The recovery test is evidenced by the most recent exercise record. The mobile standard is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is traced to the ticket history for the period. The vendor register is validated by the dependency map. Records are retained only as long as the schedule requires.

The threat model is reviewed against the quarterly review notes. The continuity plan is compared with the approved design baseline. The metric set is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The identity lifecycle is compared with the ticket history for the period. The change process is documented alongside the previous year's assessment. Third parties must demonstrate the control before access is granted.

The threat model is reconciled with the evidence pack held by the owner. The threat model is traced to the approved design baseline. The access review process is reviewed against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

15. The endpoint baseline

The email authentication record is compared with the dependency map. Each administrative account is measured against the commissioning document. The monitoring pipeline is measured against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is measured against the ticket history for the period. The patch calendar is reviewed against the commissioning document. Third parties must demonstrate the control before access is granted.

The metric set is compared with the ticket history for the period. The vendor register is checked against the previous year's assessment. The encryption standard is checked against the commissioning document. Metrics are reported as trends rather than single data points.