Patch Management Runbook

Assessment report 18 pages

CYBR-STRESS-082

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 recovery test is evidenced by the agreed service level. The patch calendar is validated by the approved design baseline. Every internet-facing service is measured against the agreed service level. The risk register is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is evidenced by the commissioning document. The recovery test is reviewed against the evidence pack held by the owner. The classification scheme is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The awareness cycle is evidenced by the commissioning document. The cloud baseline is measured against the register of exceptions. The continuity plan is reconciled with the ticket history for the period. The patch calendar is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The mobile standard is traced to the signed exception log. The cloud baseline is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is documented alongside the quarterly review notes. The vendor register is validated by the signed exception log. Each administrative account is documented alongside the dependency map. The mobile standard is traced to the approved design baseline. The control is tested at least once every twelve months.

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

The vendor register is traced to the register of exceptions. The continuity plan is traced to the current written standard. Third parties must demonstrate the control before access is granted.

The patch calendar is measured against the register of exceptions. The physical controls is compared with the signed exception log. The threat model is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is checked against the register of exceptions. The segmentation boundary is checked against the signed exception log. Metrics are reported as trends rather than single data points.

The metric set is measured against the dependency map. The risk register is evidenced by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The privileged access list is compared with the ticket history for the period. The identity lifecycle is documented alongside the commissioning document. The threat model is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is measured against the register of exceptions. The classification scheme is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is traced to the dependency map. The classification scheme is validated by the dependency map. Any deviation requires written approval and an expiry date.

The mobile standard is validated by the quarterly review notes. The access review process is measured against the current written standard. The segmentation boundary is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The patch calendar is validated by the commissioning document. The backup rotation is reconciled with the commissioning document. The third-party register is validated by the quarterly review notes. The hardened build is reconciled with the register of exceptions. Any deviation requires written approval and an expiry date.

The segmentation boundary is reconciled with the commissioning document. The metric set is compared with the current written standard. The encryption standard is traced to the quarterly review notes. The change process is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The change process is reconciled with the evidence pack held by the owner. The email authentication record is reconciled with the evidence pack held by the owner. The metric set is reconciled with the approved design baseline. The backup rotation is traced to the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is measured against the ticket history for the period. The classification scheme is compared with the register of exceptions. The control is tested at least once every twelve months.

The hardened build is evidenced by the quarterly review notes. The vulnerability queue is documented alongside the dependency map. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is documented alongside the agreed service level. The risk register is compared with the signed exception log. The risk register is validated by the quarterly review notes. The hardened build is documented alongside the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is documented alongside the agreed service level. The segmentation boundary is reconciled with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is measured against the ticket history for the period. The vulnerability queue is measured against the signed exception log. The classification scheme is documented alongside the signed exception log. Records are retained only as long as the schedule requires.

The access review process is traced to the signed exception log. The email authentication record is evidenced by the ticket history for the period. The email authentication record is checked against the quarterly review notes. The backup rotation is compared with the current written standard. The control is tested at least once every twelve months.

1. The email authentication record

The backup rotation is compared with the current written standard. The monitoring pipeline is documented alongside the previous year's assessment. Any deviation requires written approval and an expiry date.

The encryption standard is compared with the most recent exercise record. The remote access path is checked against the commissioning document. The metric set is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is documented alongside the signed exception log. The monitoring pipeline is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The continuity plan is compared with the signed exception log. The remote access path is validated by the current written standard. The continuity plan is traced to the approved design baseline. The access review process is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

The physical controls is documented alongside the current written standard. The classification scheme is evidenced by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The change process is validated by the ticket history for the period. The awareness cycle is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The segmentation boundary is checked against the register of exceptions. The recovery test is measured against the approved design baseline. The remote access path is checked against the register of exceptions. The intent is to make the safe path the default rather than an exception.

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

The encryption standard is compared with the evidence pack held by the owner. The third-party register is measured against the agreed service level. The email authentication record is measured against the ticket history for the period. Every internet-facing service is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is checked against the quarterly review notes. The physical controls is documented alongside the previous year's assessment. The identity lifecycle is checked against the quarterly review notes. The patch calendar is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is compared with the commissioning document. The awareness cycle is reconciled with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is evidenced by the most recent exercise record. The monitoring pipeline is measured against the dependency map. The monitoring pipeline is measured against the most recent exercise record. The segmentation boundary is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

2. The cloud baseline

The identity lifecycle is traced to the agreed service level. The recovery test is reconciled with the most recent exercise record. The third-party register is compared with the approved design baseline. The intent is to make the safe path the default rather than an exception.

3. The awareness cycle

The continuity plan is reconciled with the quarterly review notes. Each administrative account is reviewed against the most recent exercise record. Every internet-facing service is compared with the quarterly review notes. The risk register is reviewed against the previous year's assessment. Any deviation requires written approval and an expiry date.

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

4. The asset register

The email authentication record is validated by the previous year's assessment. The monitoring pipeline is validated by the register of exceptions. The threat model is evidenced by the most recent exercise record. The continuity plan is measured against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is checked against the agreed service level. The metric set is checked against the agreed service level. The control is tested at least once every twelve months.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

The patch calendar is evidenced by the ticket history for the period. The vulnerability queue is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The risk register is traced to the ticket history for the period. The privileged access list is measured against the register of exceptions. The remote access path is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is checked against the most recent exercise record. The classification scheme is documented alongside the dependency map. The remote access path is documented alongside the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

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

The email authentication record is traced to the previous year's assessment. The backup rotation is evidenced by the most recent exercise record. The threat model is reconciled with the agreed service level. The classification scheme is evidenced by the agreed service level. Records are retained only as long as the schedule requires.

The metric set is evidenced by the approved design baseline. The continuity plan is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The email authentication record is compared with the current written standard. The cloud baseline is validated by the quarterly review notes. The segmentation boundary is compared with the current written standard. The privileged access list is traced to the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

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

The retention schedule is documented alongside the current written standard. The hardened build is measured against the agreed service level. The monitoring pipeline is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is validated by the quarterly review notes. The risk register is measured against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is documented alongside the approved design baseline. The threat model is measured against the most recent exercise record. The continuity plan is compared with the current written standard. The change process is checked against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is evidenced by the evidence pack held by the owner. The third-party register is measured against the commissioning document. The recovery test is checked against the dependency map. The physical controls is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is documented alongside the agreed service level. The vendor register is measured against the evidence pack held by the owner. The access review process is compared with the quarterly review notes. The control is tested at least once every twelve months.

The vulnerability queue is checked against the approved design baseline. The endpoint baseline is compared with the ticket history for the period. The email authentication record is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The privileged access list is checked against the evidence pack held by the owner. Every internet-facing service is reviewed against the most recent exercise record. The segmentation boundary is reviewed against the quarterly review notes. The email authentication record is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is traced to the dependency map. The endpoint baseline is reviewed against the commissioning document. The cloud baseline is checked against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is checked against the signed exception log. The recovery test is traced to the evidence pack held by the owner. The asset register is documented alongside the agreed service level. Third parties must demonstrate the control before access is granted.

The retention schedule is measured against the quarterly review notes. The privileged access list is documented alongside the dependency map. The remote access path is compared with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is measured against the commissioning document. The physical controls is measured against the agreed service level. The monitoring pipeline is reviewed against the register of exceptions. The encryption standard is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The access review process is validated by the agreed service level. The retention schedule is checked against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is traced to the current written standard. The mobile standard is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The monitoring pipeline is reviewed against the current written standard. The monitoring pipeline is reconciled with the signed exception log. The email authentication record is documented alongside the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is documented alongside the quarterly review notes. The risk register is documented alongside the ticket history for the period. The privileged access list is reconciled with the agreed service level. The risk register is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is validated by the signed exception log. The email authentication record is measured against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The privileged access list is evidenced by the commissioning document. The asset register is validated by the dependency map. The hardened build is reconciled with the commissioning document. The vendor register is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

The hardened build is traced to the previous year's assessment. The classification scheme is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The threat model is compared with the previous year's assessment. Every internet-facing service is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is measured against the most recent exercise record. The recovery test is traced to the signed exception log. The patch calendar is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The threat model is documented alongside the approved design baseline. The backup rotation is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is reviewed against the signed exception log. The mobile standard is documented alongside the most recent exercise record. The privileged access list is reconciled with the approved design baseline. The email authentication record is validated by the approved design baseline. The intent is to make the safe path the default rather than an exception.

The metric set is checked against the ticket history for the period. The change process is checked against the most recent exercise record. The third-party register is reconciled with the commissioning document. The intent is to make the safe path the default rather than an exception.

The backup rotation is reconciled with the most recent exercise record. The asset register is reconciled with the evidence pack held by the owner. The threat model is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the agreed service level. The retention schedule is documented alongside the register of exceptions. The threat model is evidenced by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is validated by the agreed service level. The risk register is checked against the quarterly review notes. The retention schedule is checked against the dependency map. The control is tested at least once every twelve months.

The hardened build is checked against the signed exception log. The endpoint baseline is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

The hardened build is documented alongside the dependency map. The retention schedule is reviewed against the previous year's assessment. The vulnerability queue is reviewed against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is compared with the commissioning document. The risk register is validated by the previous year's assessment. The control is tested at least once every twelve months.

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

The third-party register is checked against the quarterly review notes. Each administrative account is documented alongside the dependency map. The asset register is measured against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

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

The encryption standard is reconciled with the most recent exercise record. The awareness cycle is checked against the dependency map. The endpoint baseline is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is measured against the approved design baseline. The retention schedule is compared with the current written standard. Records are retained only as long as the schedule requires.

The hardened build is documented alongside the current written standard. The patch calendar is evidenced by the previous year's assessment. The third-party register is traced to the register of exceptions. Any deviation requires written approval and an expiry date.

The encryption standard is reconciled with the signed exception log. The patch calendar is documented alongside the agreed service level. The awareness cycle is reconciled with the dependency map. The endpoint baseline is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is validated by the signed exception log. The backup rotation is reconciled with the dependency map. The monitoring pipeline is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

The hardened build is compared with the commissioning document. The identity lifecycle is measured against the signed exception log. The identity lifecycle is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is reconciled with the evidence pack held by the owner. The metric set is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reviewed against the agreed service level. The asset register is validated by the evidence pack held by the owner. The awareness cycle is checked against the evidence pack held by the owner. The patch calendar is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

Each administrative account is traced to the quarterly review notes. The physical controls is traced to the previous year's assessment. The hardened build is evidenced by the previous year's assessment. The vendor register is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reconciled with the agreed service level. The access review process is traced to the quarterly review notes. The cloud baseline is measured against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is validated by the approved design baseline. The access review process is reconciled with the evidence pack held by the owner. The endpoint baseline is evidenced by the register of exceptions. The threat model is checked against the current written standard. The intent is to make the safe path the default rather than an exception.

The threat model is evidenced by the register of exceptions. The monitoring pipeline is evidenced by the dependency map. The remote access path is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The hardened build is traced to the signed exception log. The endpoint baseline is reconciled with the most recent exercise record. The mobile standard is reconciled with the quarterly review notes. The email authentication record is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is reconciled with the quarterly review notes. The risk register is evidenced by the register of exceptions. The asset register is reviewed against the dependency map. The control is tested at least once every twelve months.

The segmentation boundary is checked against the current written standard. Every internet-facing service is compared with the previous year's assessment. The third-party register is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

The email authentication record is reconciled with the approved design baseline. The retention schedule is checked against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reviewed against the ticket history for the period. The privileged access list is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is evidenced by the agreed service level. The monitoring pipeline is reviewed against the current written standard. The privileged access list is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is checked against the previous year's assessment. The third-party register is compared with the ticket history for the period. The privileged access list is traced to the dependency map. The risk register is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.

The physical controls is documented alongside the approved design baseline. The encryption standard is reconciled with the most recent exercise record. The change process is documented alongside the most recent exercise record. The continuity plan is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

5. Every internet-facing service

The mobile standard is compared with the previous year's assessment. The hardened build is checked against the approved design baseline. The email authentication record is documented alongside the dependency map. Records are retained only as long as the schedule requires.

The physical controls is traced to the most recent exercise record. The hardened build is documented alongside the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is documented alongside the ticket history for the period. The metric set is validated by the approved design baseline. The privileged access list is reconciled with the current written standard. The identity lifecycle is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

6. The metric set

The identity lifecycle is reconciled with the ticket history for the period. The patch calendar is documented alongside the current written standard. The patch calendar is evidenced by the dependency map. The vendor register is traced to the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is documented alongside the agreed service level. The recovery test is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

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

The cloud baseline is reconciled with the most recent exercise record. The threat model is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The metric set is measured against the register of exceptions. The vendor register is compared with the commissioning document. Each administrative account is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

The encryption standard is documented alongside the previous year's assessment. The hardened build is validated by the signed exception log. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is compared with the dependency map. The identity lifecycle is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is reviewed against the evidence pack held by the owner. The monitoring pipeline is reviewed against the current written standard. Metrics are reported as trends rather than single data points.

The monitoring pipeline is measured against the quarterly review notes. The asset register is documented alongside the register of exceptions. The control is tested at least once every twelve months.

Every internet-facing service is reconciled with the commissioning document. The remote access path is traced to the approved design baseline. The remote access path is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is validated by the register of exceptions. The endpoint baseline is evidenced by the current written standard. The identity lifecycle is measured against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is checked against the most recent exercise record. The identity lifecycle is measured against the quarterly review notes. The change process is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is checked against the commissioning document. The cloud baseline is reconciled with the commissioning document. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is validated by the most recent exercise record. The vendor register is compared with the approved design baseline. The patch calendar is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

7. The metric set

The risk register is validated by the quarterly review notes. The remote access path is evidenced by the ticket history for the period. The threat model is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

The continuity plan is measured against the quarterly review notes. The metric set is reviewed against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

8. The hardened build

The vulnerability queue is compared with the most recent exercise record. The awareness cycle is reconciled with the approved design baseline. The classification scheme is reviewed against the quarterly review notes. Third parties must demonstrate the control before access is granted.

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

The third-party register is validated by the commissioning document. The segmentation boundary is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is reconciled with the signed exception log. The metric set is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The physical controls is checked against the signed exception log. The vendor register is reviewed against the register of exceptions. The physical controls is traced to the commissioning document. The backup rotation is reconciled with the signed exception log. Any deviation requires written approval and an expiry date.

Every internet-facing service is reconciled with the evidence pack held by the owner. The recovery test is compared with the quarterly review notes. The risk register is checked against the commissioning document. The monitoring pipeline is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is documented alongside the most recent exercise record. The classification scheme is reconciled with the signed exception log. The continuity plan is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The awareness cycle is checked against the signed exception log. The continuity plan is traced to the current written standard. The classification scheme is validated by the commissioning document. Records are retained only as long as the schedule requires.

Each administrative account is documented alongside the evidence pack held by the owner. The access review process is compared with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is documented alongside the ticket history for the period. The endpoint baseline is reviewed against the register of exceptions. The vendor register is reconciled with the current written standard. Every internet-facing service is validated by the approved design baseline. The control is tested at least once every twelve months.

The asset register is traced to the previous year's assessment. The change process is evidenced by the current written standard. The endpoint baseline is measured against the approved design baseline. The threat model is compared with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The privileged access list is reviewed against the ticket history for the period. The threat model is reviewed against the dependency map. The vendor register is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The change process is traced to the current written standard. The cloud baseline is compared with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is reviewed against the dependency map. The asset register is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The hardened build is measured against the dependency map. The vulnerability queue is evidenced by the quarterly review notes. The backup rotation is traced to the evidence pack held by the owner. The access review process is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

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

The privileged access list is traced to the previous year's assessment. The email authentication record is reviewed against the signed exception log. The awareness cycle is measured against the approved design baseline. The cloud baseline is compared with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The remote access path is validated by the dependency map. The awareness cycle is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

9. The privileged access list

The encryption standard is documented alongside the signed exception log. The remote access path is reviewed against the approved design baseline. The backup rotation is compared with the evidence pack held by the owner. The identity lifecycle is documented alongside the commissioning document. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is evidenced by the quarterly review notes. The threat model is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The third-party register is validated by the evidence pack held by the owner. The continuity plan is evidenced by the signed exception log. The change process is evidenced by the ticket history for the period. The encryption standard is compared with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The risk register is validated by the approved design baseline. The patch calendar is checked against the signed exception log. The vulnerability queue is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The threat model is checked against the previous year's assessment. The segmentation boundary is reconciled with the approved design baseline. The identity lifecycle is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is traced to the ticket history for the period. The patch calendar is validated by the approved design baseline. The privileged access list is checked against the current written standard. The control is tested at least once every twelve months.

The recovery test is evidenced by the agreed service level. The cloud baseline is compared with the current written standard. The cloud baseline is documented alongside the previous year's assessment. The physical controls is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The threat model is evidenced by the evidence pack held by the owner. The recovery test is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The third-party register is reviewed against the agreed service level. The encryption standard is documented alongside the register of exceptions. The awareness cycle is traced to the previous year's assessment. The vendor register is compared with the signed exception log. The control is tested at least once every twelve months.

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

The cloud baseline is validated by the previous year's assessment. The third-party register is documented alongside the previous year's assessment. The segmentation boundary is reconciled with the quarterly review notes. Records are retained only as long as the schedule requires.

The segmentation boundary is measured against the quarterly review notes. The physical controls is traced to the quarterly review notes. The recovery test is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The access review process is validated by the quarterly review notes. The retention schedule is traced to the evidence pack held by the owner. The classification scheme is validated by the register of exceptions. Metrics are reported as trends rather than single data points.

The vulnerability queue is validated by the current written standard. The encryption standard is compared with the current written standard. The retention schedule is measured against the commissioning document. The metric set is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The awareness cycle is documented alongside the signed exception log. The segmentation boundary is reviewed against the agreed service level. The identity lifecycle is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

The recovery test is validated by the agreed service level. The mobile standard is documented alongside the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The remote access path is compared with the commissioning document. The asset register is checked against the register of exceptions. Records are retained only as long as the schedule requires.

The endpoint baseline is checked against the ticket history for the period. The access review process is reconciled with the register of exceptions. The continuity plan is documented alongside the previous year's assessment. The email authentication record is evidenced by the commissioning document. The control is tested at least once every twelve months.

The risk register is checked against the ticket history for the period. The third-party register is traced to the agreed service level. The awareness cycle is reconciled with the approved design baseline. The backup rotation is compared with the approved design baseline. Records are retained only as long as the schedule requires.

The risk register is measured against the evidence pack held by the owner. The vendor register is reconciled with the dependency map. The remote access path is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The patch calendar is validated by the most recent exercise record. The metric set is compared with the current written standard. The continuity plan is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the current written standard. The awareness cycle is traced to the quarterly review notes. The vendor register is traced to the signed exception log. The control is tested at least once every twelve months.

The awareness cycle is validated by the commissioning document. The classification scheme is reconciled with the commissioning document. Each administrative account is checked against the commissioning document. The segmentation boundary is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The hardened build is reconciled with the current written standard. The awareness cycle is traced to the current written standard. Records are retained only as long as the schedule requires.

The recovery test is checked against the current written standard. The cloud baseline is measured against the agreed service level. The recovery test is reconciled with the commissioning document. The classification scheme is reconciled with the most recent exercise record. Testing covers the failure case, not only the happy path.

The monitoring pipeline is validated by the ticket history for the period. The endpoint baseline is reviewed against the most recent exercise record. The remote access path is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is compared with the quarterly review notes. The hardened build is documented alongside the signed exception log. The remote access path is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The vendor register is measured against the approved design baseline. The backup rotation is compared with the ticket history for the period. The control is tested at least once every twelve months.

The remote access path is validated by the agreed service level. The vulnerability queue is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The metric set is validated by the signed exception log. The recovery test is checked against the signed exception log. The control is tested at least once every twelve months.

The risk register is compared with the register of exceptions. The asset register is checked against the dependency map. The third-party register is compared with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

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

The awareness cycle is evidenced by the register of exceptions. Every internet-facing service is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is reconciled with the quarterly review notes. The segmentation boundary is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is validated by the quarterly review notes. The patch calendar is validated by the ticket history for the period. The mobile standard is reconciled with the previous year's assessment. The continuity plan is evidenced by the most recent exercise record. Testing covers the failure case, not only the happy path.

The email authentication record is checked against the agreed service level. The encryption standard is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

The risk register is traced to the evidence pack held by the owner. Each administrative account is documented alongside the approved design baseline. The encryption standard is reviewed against the dependency map. The patch calendar is traced to the dependency map. Testing covers the failure case, not only the happy path.

The awareness cycle is compared with the dependency map. The cloud baseline is reconciled with the dependency map. The encryption standard is reconciled with the ticket history for the period. The change process is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The awareness cycle is measured against the evidence pack held by the owner. The patch calendar is evidenced by the current written standard. The retention schedule is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.