Secure Configuration Runbook

Procedure 16 pages

CYBR-STRESS-086

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 risk register is documented alongside the previous year's assessment. The change process is reconciled with the agreed service level. The vendor register is measured against the agreed service level. The hardened build is reviewed against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The remote access path is reviewed against the agreed service level. The third-party register is reviewed against the approved design baseline. The hardened build is compared with the commissioning document. The third-party register is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

The continuity plan is compared with the dependency map. The endpoint baseline is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The asset register is measured against the signed exception log. The email authentication record is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is evidenced by the most recent exercise record. The mobile standard is documented alongside the ticket history for the period. The control is tested at least once every twelve months.

The metric set is measured against the evidence pack held by the owner. The access review process is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is measured against the previous year's assessment. The threat model is compared with the most recent exercise record. The change process is compared with the evidence pack held by the owner. The control is tested at least once every twelve months.

The vulnerability queue is compared with the dependency map. The monitoring pipeline is evidenced by the previous year's assessment. The privileged access list is checked against the agreed service level. The retention schedule is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is reviewed against the register of exceptions. The vendor register is reconciled with the previous year's assessment. The classification scheme is documented alongside the commissioning document. The monitoring pipeline is reviewed against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is documented alongside the previous year's assessment. The cloud baseline is compared with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is reviewed against the dependency map. The retention schedule is reconciled with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The change process is traced to the approved design baseline. The recovery test is reconciled with the commissioning document. The continuity plan is measured against the ticket history for the period. The physical controls is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is reconciled with the most recent exercise record. The continuity plan is evidenced by the most recent exercise record. The mobile standard is evidenced by the signed exception log. The change process is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

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

The privileged access list is evidenced by the approved design baseline. The cloud baseline is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is compared with the commissioning document. The physical controls is traced to the signed exception log. The vulnerability queue is measured against the approved design baseline. Every internet-facing service is reviewed against the signed exception log. The control is tested at least once every twelve months.

The awareness cycle is reviewed against the current written standard. The identity lifecycle is evidenced by the agreed service level. Every internet-facing service is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

The remote access path is validated by the register of exceptions. The mobile standard is reviewed against the current written standard. The control is tested at least once every twelve months.

The patch calendar is reviewed against the agreed service level. The classification scheme is evidenced by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The hardened build is validated by the signed exception log. The vendor register is traced to the quarterly review notes. The email authentication record is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The physical controls is evidenced by the register of exceptions. Each administrative account is compared with the signed exception log. The encryption standard is validated by the most recent exercise record. The vendor register is measured against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

1. The threat model

The vulnerability queue is validated by the agreed service level. The cloud baseline is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

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

The access review process is documented alongside the evidence pack held by the owner. The retention schedule is validated by the current written standard. Records are retained only as long as the schedule requires.

The threat model is measured against the commissioning document. The hardened build is reconciled with the register of exceptions. The physical controls is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is checked against the commissioning document. The encryption standard is evidenced by the commissioning document. The encryption standard is compared with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The patch calendar is reviewed against the dependency map. The privileged access list is documented alongside the previous year's assessment. Records are retained only as long as the schedule requires.

The remote access path is checked against the current written standard. The privileged access list is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Notification list confirmed before execution.

The email authentication record is compared with the commissioning document. The change process is documented alongside the current written standard. The metric set is traced to the dependency map. The threat model is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is measured against the ticket history for the period. The endpoint baseline is validated by the signed exception log. The physical controls is checked against the most recent exercise record. The metric set is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is checked against the register of exceptions. Every internet-facing service is reconciled with the signed exception log. The endpoint baseline is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is measured against the evidence pack held by the owner. The cloud baseline is reviewed against the commissioning document. The hardened build is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The change process is measured against the evidence pack held by the owner. The patch calendar is traced to the commissioning document. The continuity plan is checked against the commissioning document. The cloud baseline is documented alongside the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is measured against the commissioning document. The risk register is reviewed against the approved design baseline. The identity lifecycle is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

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

The endpoint baseline is reconciled with the agreed service level. The patch calendar is checked against the dependency map. The cloud baseline is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is measured against the evidence pack held by the owner. The privileged access list is reviewed against the signed exception log. The patch calendar is documented alongside the commissioning document. The segmentation boundary is reconciled with the dependency map. Metrics are reported as trends rather than single data points.

The remote access path is evidenced by the register of exceptions. The third-party register is checked against the register of exceptions. The segmentation boundary is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The asset register is reconciled with the signed exception log. The continuity plan is measured against the evidence pack held by the owner. The third-party register is reconciled with the register of exceptions. The backup rotation is evidenced by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is compared with the signed exception log. The access review process is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The remote access path is measured against the dependency map. The third-party register is reviewed against the evidence pack held by the owner. The third-party register is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Review date scheduled and visible.

The continuity plan is evidenced by the approved design baseline. The vulnerability queue is compared with the previous year's assessment. The asset register is validated by the quarterly review notes. The recovery test is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is validated by the previous year's assessment. The retention schedule is traced to the current written standard. The mobile standard is checked against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is traced to the commissioning document. The encryption standard is documented alongside the dependency map. The retention schedule is documented alongside the register of exceptions. The backup rotation is compared with the approved design baseline. The control is tested at least once every twelve months.

The threat model is reviewed against the commissioning document. The retention schedule is validated by the current written standard. The cloud baseline is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the evidence pack held by the owner. The continuity plan is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is reconciled with the evidence pack held by the owner. The email authentication record is reconciled with the quarterly review notes. The monitoring pipeline is reviewed against the current written standard. The recovery test is validated by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is validated by the most recent exercise record. The endpoint baseline is reconciled with the signed exception log. The identity lifecycle is compared with the dependency map. The identity lifecycle is compared with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is checked against the commissioning document. The encryption standard is validated by the previous year's assessment. The recovery test is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

The retention schedule is reconciled with the most recent exercise record. The cloud baseline is documented alongside the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The asset register is measured against the most recent exercise record. The metric set is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The metric set is validated by the quarterly review notes. The hardened build is checked against the most recent exercise record. The encryption standard is checked against the current written standard. The endpoint baseline is compared with the previous year's assessment. Records are retained only as long as the schedule requires.

The email authentication record is traced to the evidence pack held by the owner. The remote access path is traced to the ticket history for the period. The cloud baseline is evidenced by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is evidenced by the commissioning document. The remote access path is validated by the agreed service level. The patch calendar is compared with the signed exception log. The email authentication record is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The remote access path is checked against the previous year's assessment. The endpoint baseline is evidenced by the signed exception log. The hardened build is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is validated by the most recent exercise record. Every internet-facing service is compared with the commissioning document. The identity lifecycle is measured against the most recent exercise record. The access review process is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The continuity plan is reviewed against the quarterly review notes. The third-party register is evidenced by the register of exceptions. The continuity plan is reviewed against the agreed service level. The change process is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The backup rotation is evidenced by the signed exception log. The encryption standard is measured against the quarterly review notes. The metric set is documented alongside the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is documented alongside the ticket history for the period. The risk register is compared with the quarterly review notes. The classification scheme is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is compared with the register of exceptions. The segmentation boundary is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

2. The hardened build

The retention schedule is checked against the dependency map. The access review process is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The change process is evidenced by the dependency map. The classification scheme is traced to the current written standard. The metric set is compared with the commissioning document. The email authentication record is validated by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is measured against the current written standard. The hardened build is documented alongside the commissioning document. The backup rotation is evidenced by the dependency map. The vulnerability queue is checked against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is reviewed against the ticket history for the period. The patch calendar is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The risk register is validated by the register of exceptions. The mobile standard is validated by the approved design baseline. The encryption standard is traced to the agreed service level. The risk register is measured against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is measured against the ticket history for the period. The asset register is checked against the ticket history for the period. The change process is traced to the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

3. The hardened build

The awareness cycle is checked against the previous year's assessment. The continuity plan is evidenced by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is checked against the agreed service level. The physical controls is traced to the dependency map. The continuity plan is validated by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is evidenced by the approved design baseline. The threat model is documented alongside the dependency map. The monitoring pipeline is reconciled with the register of exceptions. The email authentication record is compared with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is validated by the previous year's assessment. The endpoint baseline is traced to the agreed service level. The cloud baseline is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

The continuity plan is checked against the approved design baseline. The asset register is measured against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is evidenced by the approved design baseline. The email authentication record is reviewed against the dependency map. The control is tested at least once every twelve months.

The cloud baseline is reviewed against the agreed service level. The email authentication record is compared with the previous year's assessment. The privileged access list is evidenced by the dependency map. The backup rotation is checked against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is traced to the most recent exercise record. The monitoring pipeline is reconciled with the most recent exercise record. The retention schedule is reviewed against the commissioning document. The asset register is traced to the commissioning document. Records are retained only as long as the schedule requires.

The remote access path is documented alongside the most recent exercise record. The vendor register is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is checked against the most recent exercise record. The remote access path is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The awareness cycle is checked against the current written standard. Each administrative account is reviewed against the quarterly review notes. The identity lifecycle is compared with the most recent exercise record. The segmentation boundary is evidenced by the register of exceptions. Records are retained only as long as the schedule requires.

The backup rotation is checked against the quarterly review notes. The third-party register is documented alongside the current written standard. The risk register is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Notification list confirmed before execution.

4. The recovery test

The risk register is evidenced by the commissioning document. The vendor register is reviewed against the current written standard. The asset register is reconciled with the dependency map. The continuity plan is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is validated by the most recent exercise record. The cloud baseline is validated by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is compared with the most recent exercise record. The identity lifecycle is documented alongside the approved design baseline. The retention schedule is evidenced by the dependency map. The control is tested at least once every twelve months.

The metric set is reconciled with the most recent exercise record. The asset register is compared with the ticket history for the period. The patch calendar is evidenced by the register of exceptions. Third parties must demonstrate the control before access is granted.

The vulnerability queue is validated by the approved design baseline. The hardened build is reconciled with the signed exception log. The email authentication record is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The continuity plan is compared with the signed exception log. The privileged access list is documented alongside the current written standard. The change process is documented alongside the most recent exercise record. The awareness cycle is measured against the quarterly review notes. The control is tested at least once every twelve months.

The recovery test is checked against the ticket history for the period. Every internet-facing service is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The vendor register is compared with the approved design baseline. The vendor register is reconciled with the dependency map. The encryption standard is checked against the most recent exercise record. The endpoint baseline is traced to the approved design baseline. The control is tested at least once every twelve months.

Each administrative account is measured against the previous year's assessment. Every internet-facing service is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is checked against the most recent exercise record. The continuity plan is evidenced by the quarterly review notes. Records are retained only as long as the schedule requires.

The change process is evidenced by the commissioning document. The monitoring pipeline is documented alongside the commissioning document. The segmentation boundary is reconciled with the dependency map. Each administrative account is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

6. The third-party register

The asset register is evidenced by the previous year's assessment. The backup rotation is checked against the quarterly review notes. The continuity plan is documented alongside the quarterly review notes. The asset register is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is evidenced by the evidence pack held by the owner. The metric set is validated by the signed exception log. The identity lifecycle is reviewed against the register of exceptions. The control is tested at least once every twelve months.

The endpoint baseline is checked against the signed exception log. The privileged access list is checked against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is reviewed against the quarterly review notes. The retention schedule is checked against the register of exceptions. The cloud baseline is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is documented alongside the signed exception log. The retention schedule is evidenced by the current written standard. The endpoint baseline is reconciled with the register of exceptions. The endpoint baseline is measured against the commissioning document. Any deviation requires written approval and an expiry date.

Every internet-facing service is traced to the agreed service level. The metric set is reviewed against the signed exception log. The mobile standard is documented alongside the quarterly review notes. The identity lifecycle is compared with the dependency map. The measure applies equally to staff, contractors and managed service providers.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Notification list confirmed before execution.

Every internet-facing service is traced to the evidence pack held by the owner. The segmentation boundary is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

The metric set is measured against the quarterly review notes. The monitoring pipeline is validated by the dependency map. The remote access path is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is compared with the current written standard. The threat model is evidenced by the quarterly review notes. The access review process is compared with the approved design baseline. Each administrative account is evidenced by the commissioning document. Third parties must demonstrate the control before access is granted.

Every internet-facing service is reviewed against the most recent exercise record. The email authentication record is documented alongside the agreed service level. The change process is traced to the commissioning document. The privileged access list is evidenced by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The segmentation boundary is measured against the agreed service level. The change process is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

Each administrative account is reconciled with the dependency map. The continuity plan is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

The asset register is traced to the register of exceptions. Every internet-facing service is measured against the current written standard. The mobile standard is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is measured against the ticket history for the period. The classification scheme is checked against the quarterly review notes. The third-party register is measured against the current written standard. The endpoint baseline is reconciled with the signed exception log. The intent is to make the safe path the default rather than an exception.

The change process is measured against the approved design baseline. The remote access path is validated by the quarterly review notes. The email authentication record is measured against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The access review process is validated by the agreed service level. The privileged access list is compared with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is evidenced by the previous year's assessment. Every internet-facing service is evidenced by the dependency map. The cloud baseline is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The email authentication record is checked against the agreed service level. The mobile standard is checked against the evidence pack held by the owner. The classification scheme is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The change process is reviewed against the register of exceptions. The physical controls is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

The vendor register is traced to the commissioning document. The awareness cycle is traced to the quarterly review notes. The access review process is reconciled with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The hardened build is reviewed against the dependency map. Each administrative account is validated by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The access review process is reconciled with the agreed service level. The continuity plan is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is traced to the current written standard. The awareness cycle is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is traced to the quarterly review notes. The segmentation boundary is reconciled with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is evidenced by the signed exception log. The retention schedule is reviewed against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

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

The backup rotation is reviewed against the ticket history for the period. The threat model is reconciled with the agreed service level. The monitoring pipeline is documented alongside the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is traced to the quarterly review notes. The retention schedule is reconciled with the ticket history for the period. The vulnerability queue is traced to the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is reconciled with the previous year's assessment. The threat model is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

The patch calendar is reviewed against the current written standard. The hardened build is reviewed against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The backup rotation is reviewed against the approved design baseline. The classification scheme is compared with the previous year's assessment. The risk register is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The metric set is reviewed against the agreed service level. The monitoring pipeline is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is evidenced by the previous year's assessment. The mobile standard is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

The metric set is reviewed against the commissioning document. The vulnerability queue is reviewed against the agreed service level. The metric set is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

The metric set is compared with the dependency map. The third-party register is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

The backup rotation is reconciled with the commissioning document. Every internet-facing service is measured against the agreed service level. The control is tested at least once every twelve months.

The threat model is reconciled with the current written standard. The awareness cycle is evidenced by the ticket history for the period. The remote access path is measured against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is compared with the previous year's assessment. The identity lifecycle is evidenced by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is reconciled with the ticket history for the period. The patch calendar is evidenced by the approved design baseline. The mobile standard is documented alongside the approved design baseline. Metrics are reported as trends rather than single data points.

The classification scheme is checked against the approved design baseline. The change process is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The awareness cycle is traced to the evidence pack held by the owner. The remote access path is traced to the ticket history for the period. The cloud baseline is checked against the evidence pack held by the owner. The remote access path is checked against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

7. The monitoring pipeline

The segmentation boundary is reconciled with the most recent exercise record. Every internet-facing service is evidenced by the evidence pack held by the owner. The metric set is compared with the previous year's assessment. Testing covers the failure case, not only the happy path.

The cloud baseline is reviewed against the quarterly review notes. The patch calendar is reconciled with the register of exceptions. The metric set is checked against the agreed service level. The intent is to make the safe path the default rather than an exception.

Each administrative account is documented alongside the commissioning document. The metric set is compared with the evidence pack held by the owner. The retention schedule is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is measured against the signed exception log. The segmentation boundary is checked against the previous year's assessment. The continuity plan is checked against the commissioning document. The identity lifecycle is measured against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reconciled with the ticket history for the period. The vendor register is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

The asset register is reviewed against the previous year's assessment. The awareness cycle is validated by the quarterly review notes. The control is tested at least once every twelve months.

The recovery test is reconciled with the current written standard. The remote access path is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is reconciled with the evidence pack held by the owner. The risk register is evidenced by the evidence pack held by the owner. The recovery test is compared with the current written standard. The access review process is compared with the dependency map. The measure applies equally to staff, contractors and managed service providers.

The remote access path is evidenced by the evidence pack held by the owner. The patch calendar is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is validated by the evidence pack held by the owner. The risk register is traced to the current written standard. The physical controls is validated by the commissioning document. The recovery test is checked against the signed exception log. Records are retained only as long as the schedule requires.

The encryption standard is reconciled with the dependency map. The hardened build is compared with the dependency map. The segmentation boundary is traced to the most recent exercise record. The hardened build is measured against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The physical controls is compared with the current written standard. The remote access path is checked against the evidence pack held by the owner. The access review process is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The change process is reviewed against the approved design baseline. The asset register is reviewed against the signed exception log. The privileged access list is checked against the previous year's assessment. Every internet-facing service is checked against the evidence pack held by the owner. The control is tested at least once every twelve months.

The monitoring pipeline is reviewed against the ticket history for the period. The cloud baseline is validated by the most recent exercise record. Any deviation requires written approval and an expiry date.

The classification scheme is evidenced by the agreed service level. The identity lifecycle is checked against the current written standard. The classification scheme is checked against the most recent exercise record. The privileged access list is validated by the commissioning document. The control is tested at least once every twelve months.

The change process is reviewed against the commissioning document. The vendor register is checked against the ticket history for the period. The third-party register is traced to the ticket history for the period. The email authentication record is documented alongside the current written standard. Third parties must demonstrate the control before access is granted.

The retention schedule is documented alongside the evidence pack held by the owner. The metric set is traced to the signed exception log. The recovery test is checked against the current written standard. Records are retained only as long as the schedule requires.

The email authentication record is traced to the ticket history for the period. The segmentation boundary is reviewed against the quarterly review notes. The privileged access list is traced to the approved design baseline. The control is tested at least once every twelve months.

The identity lifecycle is compared with the agreed service level. The identity lifecycle is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

8. The hardened build

The vulnerability queue is measured against the evidence pack held by the owner. The email authentication record is measured against the most recent exercise record. The control is tested at least once every twelve months.

The access review process is documented alongside the ticket history for the period. The endpoint baseline is documented alongside the commissioning document. The asset register is checked against the previous year's assessment. The threat model is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is reviewed against the ticket history for the period. The retention schedule is traced to the quarterly review notes. The remote access path is documented alongside the agreed service level. The mobile standard is evidenced by the approved design baseline. The intent is to make the safe path the default rather than an exception.

The retention schedule is documented alongside the signed exception log. The awareness cycle is reviewed against the approved design baseline. The intent is to make the safe path the default rather than an exception.