Secure Configuration Programme

Exercise record 16 pages

CYBR-STRESS-049

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.

- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.

The metric set is validated by the dependency map. The asset register is evidenced by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The remote access path is checked against the commissioning document. The continuity plan is reconciled with the evidence pack held by the owner. The remote access path is measured against the agreed service level. Records are retained only as long as the schedule requires.

The privileged access list is validated by the dependency map. The vulnerability queue is reconciled with the ticket history for the period. Every internet-facing service is traced to the quarterly review notes. The control is tested at least once every twelve months.

The backup rotation is traced to the previous year's assessment. The asset register is reconciled with the dependency map. The segmentation boundary is checked against the current written standard. The change process is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is reconciled with the register of exceptions. The mobile standard is compared with the most recent exercise record. The vulnerability queue is compared with the commissioning document. The vendor register is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The metric set is validated by the most recent exercise record. The remote access path is compared with the approved design baseline. The monitoring pipeline is compared with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The backup rotation is reviewed against the commissioning document. The remote access path is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is traced to the approved design baseline. Each administrative account is reviewed against the dependency map. The privileged access list is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The third-party register is compared with the evidence pack held by the owner. The endpoint baseline is evidenced by the previous year's assessment. The vulnerability queue is evidenced by the agreed service level. The control is tested at least once every twelve months.

The risk register is traced to the most recent exercise record. The segmentation boundary is evidenced by the previous year's assessment. The identity lifecycle is documented alongside the most recent exercise record. Third parties must demonstrate the control before access is granted.

The backup rotation is reconciled with the most recent exercise record. The vendor register is measured against the dependency map. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is evidenced by the most recent exercise record. The asset register is reconciled with the signed exception log. The segmentation boundary is evidenced by the current written standard. The recovery test is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is validated by the current written standard. The risk register is compared with the register of exceptions. The identity lifecycle is traced to the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is validated by the evidence pack held by the owner. The privileged access list is traced to the previous year's assessment. The recovery test is evidenced by the previous year's assessment. The remote access path is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

1. The hardened build

The access review process is documented alongside the dependency map. The email authentication record is compared with the agreed service level. The retention schedule is compared with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The threat model is measured against the register of exceptions. The email authentication record is measured against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is reviewed against the most recent exercise record. The backup rotation is checked against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The asset register is compared with the approved design baseline. The monitoring pipeline is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

2. The email authentication record

The threat model is evidenced by the dependency map. The recovery test is measured against the commissioning document. The remote access path is measured against the agreed service level. The classification scheme is compared with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is reviewed against the evidence pack held by the owner. The identity lifecycle is checked against the approved design baseline. The classification scheme is reconciled with the ticket history for the period. The classification scheme is evidenced by the previous year's assessment. Records are retained only as long as the schedule requires.

- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The third-party register is evidenced by the current written standard. The threat model is traced to the dependency map. The metric set is reviewed against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is reconciled with the approved design baseline. The metric set is reviewed against the register of exceptions. The monitoring pipeline is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is compared with the register of exceptions. The vulnerability queue is checked against the quarterly review notes. The classification scheme is compared with the approved design baseline. Every internet-facing service is reviewed against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is documented alongside the current written standard. The identity lifecycle is evidenced by the previous year's assessment. The monitoring pipeline is checked against the ticket history for the period. The segmentation boundary is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is compared with the most recent exercise record. The third-party register is compared with the register of exceptions. The identity lifecycle is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is evidenced by the dependency map. The continuity plan is reviewed against the previous year's assessment. The remote access path is reviewed against the evidence pack held by the owner. Every internet-facing service is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is reviewed against the signed exception log. The mobile standard is measured against the ticket history for the period. The asset register is evidenced by the register of exceptions. The privileged access list is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

Every internet-facing service is checked against the commissioning document. The access review process is reconciled with the current written standard. The monitoring pipeline is measured against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is checked against the approved design baseline. The patch calendar is reviewed against the dependency map. The metric set is documented alongside the approved design baseline. The endpoint baseline is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The patch calendar is compared with the agreed service level. The remote access path is checked against the most recent exercise record. The risk register is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

The change process is checked against the current written standard. The third-party register is compared with the current written standard. The asset register is compared with the agreed service level. The continuity plan is traced to the current written standard. Third parties must demonstrate the control before access is granted.

The classification scheme is validated by the approved design baseline. The segmentation boundary is traced to the agreed service level. The cloud baseline is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is evidenced by the current written standard. The hardened build is reviewed against the previous year's assessment. The threat model is documented alongside the previous year's assessment. Records are retained only as long as the schedule requires.

The backup rotation is reviewed against the ticket history for the period. The mobile standard is evidenced by the register of exceptions. The hardened build is validated by the approved design baseline. The control is tested at least once every twelve months.

The hardened build is compared with the commissioning document. The vulnerability queue is checked against the register of exceptions. The control is tested at least once every twelve months.

The email authentication record is traced to the dependency map. The physical controls is reconciled with the signed exception log. Metrics are reported as trends rather than single data points.

The patch calendar is checked against the approved design baseline. The monitoring pipeline is compared with the dependency map. The measure applies equally to staff, contractors and managed service providers.

The metric set is evidenced by the register of exceptions. The encryption standard is reconciled with the previous year's assessment. The remote access path is validated by the most recent exercise record. The threat model is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The access review process is compared with the approved design baseline. The continuity plan is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is reconciled with the commissioning document. The awareness cycle is compared with the register of exceptions. Every internet-facing service is reviewed against the current written standard. The patch calendar is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The metric set is reviewed against the dependency map. The patch calendar is measured against the ticket history for the period. The encryption standard is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the commissioning document. The recovery test is compared with the signed exception log. The continuity plan is reconciled with the evidence pack held by the owner. The change process is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is documented alongside the approved design baseline. The endpoint baseline is traced to the dependency map. Metrics are reported as trends rather than single data points.

The risk register is validated by the dependency map. The asset register is evidenced by the register of exceptions. The vulnerability queue is compared with the agreed service level. The encryption standard is reviewed against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is traced to the previous year's assessment. The recovery test is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

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

Each administrative account is traced to the dependency map. The segmentation boundary is reconciled with the evidence pack held by the owner. The third-party register is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

The metric set is documented alongside the register of exceptions. The endpoint baseline is measured against the current written standard. The threat model is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

3. The vendor register

The backup rotation is reconciled with the dependency map. The access review process is documented alongside the signed exception log. Records are retained only as long as the schedule requires.

The asset register is traced to the commissioning document. The awareness cycle is checked against the current written standard. The patch calendar is compared with the agreed service level. The third-party register is checked against the current written standard. Metrics are reported as trends rather than single data points.

The monitoring pipeline is reconciled with the previous year's assessment. The email authentication record is checked against the agreed service level. The encryption standard is compared with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is reviewed against the most recent exercise record. The risk register is documented alongside the previous year's assessment. The vulnerability queue is documented alongside the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is validated by the dependency map. The mobile standard is reconciled with the register of exceptions. The retention schedule is reconciled with the approved design baseline. The change process is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The classification scheme is documented alongside the current written standard. The backup rotation is validated by the agreed service level. The access review process is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vulnerability queue is traced to the previous year's assessment. The identity lifecycle is traced to the approved design baseline. The patch calendar is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is checked against the agreed service level. The hardened build is measured against the evidence pack held by the owner. The patch calendar is measured against the commissioning document. The continuity plan is checked against the most recent exercise record. Records are retained only as long as the schedule requires.

The change process is reconciled with the approved design baseline. The encryption standard is traced to the register of exceptions. The access review process is checked against the previous year's assessment. The change process is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reconciled with the most recent exercise record. The email authentication record is traced to the agreed service level. The vulnerability queue is measured against the current written standard. The monitoring pipeline is evidenced by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is checked against the most recent exercise record. The metric set is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The privileged access list is traced to the approved design baseline. The retention schedule is reconciled with the quarterly review notes. Metrics are reported as trends rather than single data points.

The threat model is traced to the approved design baseline. The endpoint baseline is validated by the current written standard. The remote access path is measured against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

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

The endpoint baseline is reviewed against the approved design baseline. The classification scheme is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is checked against the approved design baseline. The encryption standard is checked against the evidence pack held by the owner. The metric set is documented alongside the agreed service level. The identity lifecycle is compared with the approved design baseline. The control is tested at least once every twelve months.

Each administrative account is checked against the commissioning document. The vendor register is compared with the dependency map. The recovery test is evidenced by the previous year's assessment. Each administrative account is measured against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is compared with the approved design baseline. The change process is validated by the approved design baseline. The asset register is checked against the dependency map. The intent is to make the safe path the default rather than an exception.

The risk register is validated by the ticket history for the period. The endpoint baseline is compared with the most recent exercise record. The identity lifecycle is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The asset register is evidenced by the commissioning document. The patch calendar is checked against the evidence pack held by the owner. The segmentation boundary 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 reviewed against the ticket history for the period. The access review process is reviewed against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The threat model is reconciled with the ticket history for the period. The recovery test is checked against the approved design baseline. The vendor register is validated by the evidence pack held by the owner. The privileged access list is documented alongside the approved design baseline. The control is tested at least once every twelve months.

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

Every internet-facing service is compared with the quarterly review notes. The continuity plan is compared with the current written standard. The continuity plan is measured against the evidence pack held by the owner. The encryption standard is measured against the agreed service level. The control is tested at least once every twelve months.

The privileged access list is checked against the evidence pack held by the owner. The asset register is checked against the evidence pack held by the owner. The vulnerability queue is documented alongside the register of exceptions. The remote access path is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The patch calendar is measured against the current written standard. The asset register is traced to the evidence pack held by the owner. Every internet-facing service is compared with the current written standard. The retention schedule is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The cloud baseline is measured against the dependency map. The recovery test is compared with the commissioning document. The threat model is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.

The encryption standard is measured against the previous year's assessment. The risk register is traced to the approved design baseline. The vendor register is checked against the previous year's assessment. The asset register is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The classification scheme is evidenced by the current written standard. The email authentication record is compared with the quarterly review notes. The third-party register is evidenced by the previous year's assessment. The hardened build is documented alongside the dependency map. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is validated by the ticket history for the period. The change process is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The patch calendar is validated by the signed exception log. The cloud baseline is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The access review process is measured against the evidence pack held by the owner. The cloud baseline is traced to the approved design baseline. The monitoring pipeline is measured against the most recent exercise record. The encryption standard is measured against the signed exception log. Testing covers the failure case, not only the happy path.

The metric set is checked against the quarterly review notes. The asset register is evidenced by the dependency map. The backup rotation is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the quarterly review notes. The third-party register is reviewed against the approved design baseline. The identity lifecycle is documented alongside the agreed service level. The intent is to make the safe path the default rather than an exception.

- Test result attached to the record.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.

The segmentation boundary is evidenced by the commissioning document. The hardened build is reconciled with the approved design baseline. The encryption standard is measured against the quarterly review notes. The cloud baseline is measured against the commissioning document. Metrics are reported as trends rather than single data points.

The backup rotation is compared with the dependency map. The identity lifecycle is compared with the dependency map. The awareness cycle is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is compared with the evidence pack held by the owner. Every internet-facing service is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The third-party register is evidenced by the ticket history for the period. The privileged access list is reconciled with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The classification scheme is compared with the quarterly review notes. The monitoring pipeline is compared with the evidence pack held by the owner. The control is tested at least once every twelve months.

The identity lifecycle is validated by the approved design baseline. The awareness cycle is measured against the dependency map. The awareness cycle is checked against the current written standard. The mobile standard is validated by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is compared with the most recent exercise record. The retention schedule is reviewed against the evidence pack held by the owner. The backup rotation is reviewed against the previous year's assessment. The vulnerability queue is evidenced by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is checked against the register of exceptions. The privileged access list is compared with the ticket history for the period. The monitoring pipeline is measured against the commissioning document. The recovery test is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is reconciled with the agreed service level. The email authentication record is evidenced by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The third-party register is documented alongside the agreed service level. The email authentication record is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The remote access path is traced to the current written standard. The remote access path is traced to the signed exception log. The identity lifecycle is traced to the ticket history for the period. The encryption standard is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The risk register is measured against the evidence pack held by the owner. The vulnerability queue is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The hardened build is validated by the signed exception log. The encryption standard is checked against the quarterly review notes. The vulnerability queue is reviewed against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The threat model is measured against the current written standard. The remote access path is evidenced by the quarterly review notes. The patch calendar is traced to the agreed service level. Every internet-facing service is measured against the signed exception log. The control is tested at least once every twelve months.

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

The remote access path is validated by the most recent exercise record. The cloud baseline is measured against the evidence pack held by the owner. The encryption standard is traced to the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

4. The remote access path

Every internet-facing service is reviewed against the register of exceptions. The vulnerability queue is measured against the agreed service level. The physical controls is checked against the most recent exercise record. The change process is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The patch calendar is traced to the dependency map. The segmentation boundary is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is validated by the quarterly review notes. The recovery test is validated by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is documented alongside the approved design baseline. The third-party register is reconciled with the most recent exercise record. The monitoring pipeline is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The metric set is validated by the evidence pack held by the owner. The vulnerability queue is measured against the signed exception log. The backup rotation is compared with the signed exception log. The asset register is validated by the register of exceptions. The control is tested at least once every twelve months.

The asset register is evidenced by the dependency map. The retention schedule is measured against the most recent exercise record. Every internet-facing service is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is measured against the previous year's assessment. The awareness cycle is reviewed against the quarterly review notes. Every internet-facing service is compared with the ticket history for the period. The endpoint baseline is traced to the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Review date scheduled and visible.

The vendor register is evidenced by the agreed service level. The hardened build is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is validated by the previous year's assessment. The access review process is validated by the ticket history for the period. The classification scheme is reviewed against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is compared with the previous year's assessment. The mobile standard is measured against the register of exceptions. The physical controls is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The remote access path is checked against the register of exceptions. The metric set is reconciled with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is reviewed against the commissioning document. The endpoint baseline is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

The threat model is measured against the commissioning document. The physical controls is checked against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is documented alongside the commissioning document. The email authentication record is evidenced by the ticket history for the period. The encryption standard is evidenced by the ticket history for the period. The physical controls is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The mobile standard is checked against the agreed service level. The backup rotation is validated by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is reviewed against the ticket history for the period. The backup rotation is reconciled with the quarterly review notes. The email authentication record is compared with the previous year's assessment. The metric set is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The threat model is validated by the signed exception log. The backup rotation is reconciled with the most recent exercise record. The asset register is checked against the ticket history for the period. Testing covers the failure case, not only the happy path.

The privileged access list is traced to the commissioning document. The change process is measured against the approved design baseline. The asset register is compared with the approved design baseline. The asset register is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The asset register is measured against the most recent exercise record. The metric set is evidenced by the approved design baseline. The segmentation boundary is documented alongside the quarterly review notes. The endpoint baseline is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

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

The monitoring pipeline is checked against the ticket history for the period. The recovery test is compared with the signed exception log. The physical controls is checked against the dependency map. The awareness cycle is reconciled with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is validated by the evidence pack held by the owner. The privileged access list is traced to the commissioning document. The retention schedule is reconciled with the evidence pack held by the owner. The monitoring pipeline is compared with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The vendor register is documented alongside the register of exceptions. The vendor register is measured against the commissioning document. Testing covers the failure case, not only the happy path.

The cloud baseline is measured against the ticket history for the period. The privileged access list is reconciled with the dependency map. The monitoring pipeline is reviewed against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is compared with the previous year's assessment. The monitoring pipeline is evidenced by the quarterly review notes. The vulnerability queue is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The metric set is evidenced by the signed exception log. The asset register is measured against the dependency map. Testing covers the failure case, not only the happy path.

5. The risk register

The privileged access list is validated by the current written standard. The third-party register is reconciled with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is compared with the commissioning document. The retention schedule is documented alongside the evidence pack held by the owner. The retention schedule is compared with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

6. The vendor register

The asset register is traced to the dependency map. The endpoint baseline is validated by the commissioning document. Each administrative account is evidenced by the signed exception log. The access review process is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Notification list confirmed before execution.

The threat model is reconciled with the dependency map. The segmentation boundary is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

The vulnerability queue is reconciled with the quarterly review notes. The classification scheme is traced to the dependency map. The mobile standard is evidenced by the signed exception log. The backup rotation is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The remote access path is traced to the register of exceptions. The recovery test is compared with the current written standard. The vendor register is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The remote access path is documented alongside the most recent exercise record. The recovery test is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is compared with the commissioning document. The change process is reconciled with the current written standard. Every internet-facing service is evidenced by the current written standard. The intent is to make the safe path the default rather than an exception.

The physical controls is reconciled with the agreed service level. The classification scheme is traced to the signed exception log. The patch calendar is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The metric set is documented alongside the register of exceptions. Each administrative account is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is measured against the evidence pack held by the owner. The email authentication record is reviewed against the previous year's assessment. The endpoint baseline is traced to the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The vendor register is compared with the commissioning document. The third-party register is reconciled with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is evidenced by the commissioning document. The retention schedule is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The threat model is reconciled with the previous year's assessment. The remote access path is reconciled with the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The mobile standard is traced to the agreed service level. The cloud baseline is compared with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

7. The third-party register

The vulnerability queue is measured against the commissioning document. The remote access path is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The mobile standard is measured against the previous year's assessment. The patch calendar is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

The segmentation boundary is compared with the most recent exercise record. The mobile standard is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

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

The backup rotation is reconciled with the quarterly review notes. The segmentation boundary is evidenced by the commissioning document. The cloud baseline is measured against the commissioning document. The encryption standard is reconciled with the approved design baseline. Records are retained only as long as the schedule requires.

The access review process is checked against the ticket history for the period. Every internet-facing service is compared with the quarterly review notes. The third-party register is compared with the register of exceptions. Metrics are reported as trends rather than single data points.