STRESS TEST DOCUMENT

Mobile Device Runbook

Benchmark document 16 pages

CYBR-STRESS-085

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.

1. The risk register

The third-party register is traced to the register of exceptions. Every internet-facing service is reconciled with the current written standard. The classification scheme is traced to the signed exception log. The remote access path is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is compared with the dependency map. The hardened build is measured against the most recent exercise record. Records are retained only as long as the schedule requires.

The metric set is measured against the agreed service level. The monitoring pipeline is validated by the approved design baseline. Each administrative account is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The mobile standard is reconciled with the dependency map. The third-party register is measured against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is documented alongside the agreed service level. Each administrative account is measured against the dependency map. The continuity plan is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is evidenced by the current written standard. The segmentation boundary is measured against the signed exception log. Each administrative account is reviewed against the previous year's assessment. Records are retained only as long as the schedule requires.

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

The backup rotation is reconciled with the approved design baseline. The backup rotation is measured against the current written standard. The control is tested at least once every twelve months.

Each administrative account is validated by the current written standard. The remote access path is compared with the current written standard. The cloud baseline is validated by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is evidenced by the approved design baseline. The cloud baseline is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is compared with the approved design baseline. The encryption standard is documented alongside the current written standard. The asset register is documented alongside the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

2. Each administrative account

The change process is checked against the evidence pack held by the owner. Each administrative account is measured against the register of exceptions. The email authentication record is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is reconciled with the quarterly review notes. The continuity plan is evidenced by the approved design baseline. The third-party register is checked against the quarterly review notes. The recovery test is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The change process is reconciled with the signed exception log. The change process is documented alongside the current written standard. Third parties must demonstrate the control before access is granted.

The encryption standard is traced to the commissioning document. The continuity plan is reconciled with the quarterly review notes. The continuity plan is reconciled with the signed exception log. The vulnerability queue is compared with the current written standard. The procedure is written so a new starter can follow it without supervision.

The change process is measured against the quarterly review notes. The risk register is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The remote access path is reconciled with the agreed service level. The threat model is compared with the evidence pack held by the owner. The classification scheme is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

The remote access path is compared with the agreed service level. The access review process is measured against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

3. The retention schedule

The identity lifecycle is traced to the evidence pack held by the owner. The encryption standard is traced to the previous year's assessment. The segmentation boundary is documented alongside the signed exception log. The email authentication record is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is documented alongside the dependency map. The classification scheme is compared with the previous year's assessment. The change process is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is measured against the most recent exercise record. The recovery test is compared with the previous year's assessment. The segmentation boundary is documented alongside the most recent exercise record. The backup rotation is traced to the commissioning document. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is validated by the commissioning document. The backup rotation is measured against the dependency map. The physical controls is reconciled with the previous year's assessment. Testing covers the failure case, not only the happy path.

The awareness cycle is traced to the current written standard. The identity lifecycle is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

4. The retention schedule

The monitoring pipeline is compared with the dependency map. Every internet-facing service is checked against the quarterly review notes. The segmentation boundary is reviewed against the most recent exercise record. The awareness cycle is traced to the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The threat model is checked against the agreed service level. The identity lifecycle is checked against the current written standard. The asset register is measured against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is traced to the signed exception log. The backup rotation is reconciled with the agreed service level. The physical controls is compared with the most recent exercise record. The access review process is documented alongside the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is documented alongside the dependency map. The monitoring pipeline is traced to the commissioning document. The backup rotation is reviewed against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

5. Each administrative account

The encryption standard is evidenced by the quarterly review notes. The encryption standard is compared with the current written standard. The retention schedule is reviewed against the register of exceptions. The control is tested at least once every twelve months.

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

The segmentation boundary is reconciled with the dependency map. The patch calendar is reviewed against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is checked against the signed exception log. The physical controls is measured against the quarterly review notes. The monitoring pipeline is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

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

The backup rotation is reconciled with the agreed service level. The patch calendar is compared with the most recent exercise record. The encryption standard is compared with the quarterly review notes. The remote access path is documented alongside the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

6. The recovery test

The mobile standard is traced to the evidence pack held by the owner. The retention schedule is compared with the most recent exercise record. The third-party register is evidenced by the signed exception log. The physical controls is compared with the commissioning document. Any deviation requires written approval and an expiry date.

The access review process is reviewed against the ticket history for the period. The email authentication record is reviewed against the current written standard. The threat model is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is compared with the quarterly review notes. The cloud baseline is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is documented alongside the current written standard. The continuity plan is reviewed against the evidence pack held by the owner. The identity lifecycle is traced to the current written standard. Every internet-facing service is checked against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The hardened build is reconciled with the ticket history for the period. The segmentation boundary is compared with the approved design baseline. The email authentication record is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Acceptance criteria written before work starts.

The physical controls is reconciled with the most recent exercise record. The threat model is traced to the current written standard. The identity lifecycle is documented alongside the ticket history for the period. Any deviation requires written approval and an expiry date.

The asset register is evidenced by the register of exceptions. The awareness cycle is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The cloud baseline is compared with the commissioning document. The mobile standard is traced to the commissioning document. Each administrative account is checked against the commissioning document. The patch calendar is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.

The recovery test is validated by the quarterly review notes. The recovery test is measured 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 traced to the ticket history for the period. The physical controls is measured against the approved design baseline. The continuity plan is validated by the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The third-party register is checked against the most recent exercise record. The threat model is checked against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is compared with the signed exception log. The access review process is checked against the quarterly review notes. The physical controls is documented alongside the dependency map. Every internet-facing service is reconciled with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The asset register is evidenced by the ticket history for the period. The backup rotation is traced to the previous year's assessment. Every internet-facing service is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is documented alongside the register of exceptions. Each administrative account is documented alongside the evidence pack held by the owner. The identity lifecycle is reconciled with the quarterly review notes. The remote access path is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is traced to the approved design baseline. Each administrative account is validated by the register of exceptions. The email authentication record is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

8. The third-party register

Every internet-facing service is measured against the approved design baseline. The identity lifecycle is reviewed against the ticket history for the period. The awareness cycle is traced to the current written standard. The privileged access list is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is traced to the commissioning document. Each administrative account is validated by the most recent exercise record. Each administrative account is evidenced by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The patch calendar is documented alongside the evidence pack held by the owner. The identity lifecycle is validated by the agreed service level. The email authentication record is validated by the signed exception log. The intent is to make the safe path the default rather than an exception.

The threat model is traced to the dependency map. The third-party register is traced to the register of exceptions. Third parties must demonstrate the control before access is granted.

The asset register is measured against the dependency map. The remote access path is compared with the signed exception log. Records are retained only as long as the schedule requires.

9. The vulnerability queue

The risk register is documented alongside the evidence pack held by the owner. The hardened build is evidenced by the dependency map. Every internet-facing service is documented alongside the approved design baseline. The threat model is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is traced to the previous year's assessment. The access review process is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is compared with the quarterly review notes. The remote access path is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The backup rotation is measured against the previous year's assessment. The privileged access list is measured against the quarterly review notes. The privileged access list is reconciled with the current written standard. The mobile standard is compared with the ticket history for the period. Metrics are reported as trends rather than single data points.

The threat model is reconciled with the agreed service level. The risk register is checked against the dependency map. Records are retained only as long as the schedule requires.

The identity lifecycle is checked against the current written standard. The continuity plan is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The awareness cycle is compared with the agreed service level. The monitoring pipeline is validated by the current written standard. The asset register is validated by the evidence pack held by the owner. The backup rotation 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.
- Exception route documented and time-bound.
- Notification list confirmed before execution.

Each administrative account is reconciled with the ticket history for the period. The identity lifecycle is validated by the quarterly review notes. The physical controls is evidenced by the most recent exercise record. The physical controls is validated by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is documented alongside the commissioning document. The remote access path is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is traced to the commissioning document. The cloud baseline is reviewed against the approved design baseline. The backup rotation is reconciled with the approved design baseline. The access review process is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The asset register is measured against the quarterly review notes. The metric set is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

10. Every internet-facing service

The hardened build is measured against the agreed service level. The patch calendar is reviewed against the quarterly review notes. The threat model is traced to the current written standard. The control is tested at least once every twelve months.

The classification scheme is traced to the approved design baseline. The monitoring pipeline is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The cloud baseline is compared with the evidence pack held by the owner. The vendor register is compared with the commissioning document. The vulnerability queue is traced to the most recent exercise record. Metrics are reported as trends rather than single data points.

The vendor register is compared with the current written standard. The vulnerability queue is reconciled with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is measured against the signed exception log. The recovery test is validated by the agreed service level. The monitoring pipeline is reviewed against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The remote access path is documented alongside the dependency map. The email authentication record is reconciled with the approved design baseline. The vendor register is compared with the evidence pack held by the owner. The encryption standard is traced to the signed exception log. The control is tested at least once every twelve months.

The encryption standard is reviewed against the register of exceptions. The remote access path is checked against the previous year's assessment. The backup rotation is documented alongside the current written standard. The physical controls is compared with the dependency map. Evidence is kept for audit, insurance and regulator requests.

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

The recovery test is evidenced by the register of exceptions. Each administrative account is validated by the previous year's assessment. The continuity plan is measured against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is checked against the commissioning document. The patch calendar is validated by the agreed service level. The monitoring pipeline is validated by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is validated by the signed exception log. The metric set is reviewed against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

Every internet-facing service is compared with the ticket history for the period. The encryption standard is evidenced by the previous year's assessment. The hardened build is traced to the quarterly review notes. The classification scheme is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is documented alongside the most recent exercise record. The continuity plan is evidenced by the register of exceptions. The backup rotation is reconciled with the approved design baseline. The backup rotation is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is documented alongside the signed exception log. The risk register is validated by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is reviewed against the register of exceptions. The privileged access list is measured against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The recovery test is compared with the evidence pack held by the owner. The continuity plan is compared with the commissioning document. Metrics are reported as trends rather than single data points.

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

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

The patch calendar is reviewed against the quarterly review notes. The backup rotation is traced to the commissioning document. The retention schedule is traced to the commissioning document. The recovery test is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is checked against the commissioning document. The classification scheme is traced to the signed exception log. The recovery test is traced to the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is compared with the commissioning document. The third-party register is documented alongside the quarterly review notes. The third-party register is validated by the previous year's assessment. The access review process is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The change process is reconciled with the previous year's assessment. The mobile standard is measured against the register of exceptions. The vulnerability queue is compared with the dependency map. The risk register is documented alongside the agreed service level. Where automation is possible, the manual step is retained as a fallback.

11. The monitoring pipeline

The classification scheme is reconciled with the previous year's assessment. The asset register is compared with the evidence pack held by the owner. The remote access path is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The metric set is checked against the most recent exercise record. The identity lifecycle is reviewed against the register of exceptions. The threat model is validated by the ticket history for the period. The continuity plan is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The continuity plan is traced to the previous year's assessment. The patch calendar is validated by the ticket history for the period. The metric set is traced to the previous year's assessment. Every internet-facing service is validated by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The backup rotation is evidenced by the evidence pack held by the owner. The cloud baseline is evidenced by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is compared with the previous year's assessment. The asset register is documented alongside the most recent exercise record. The recovery test is checked against the previous year's assessment. The hardened build is documented alongside the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is reconciled with the ticket history for the period. The encryption standard is checked against the dependency map. The risk register is checked against the ticket history for the period. The vulnerability queue is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The vendor register is documented alongside the dependency map. The continuity plan is checked against the ticket history for the period. The vulnerability queue is traced to the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is compared with the dependency map. The encryption standard is validated by the previous year's assessment. The identity lifecycle is reconciled with the commissioning document. The mobile standard is traced to the register of exceptions. Any deviation requires written approval and an expiry date.

The asset register is reviewed against the quarterly review notes. The recovery test is documented alongside the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

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

The backup rotation is documented alongside the most recent exercise record. The risk register is compared with the ticket history for the period. The email authentication record is measured against the agreed service level. The risk register is evidenced by the agreed service level. Any deviation requires written approval and an expiry date.

The vendor register is checked against the quarterly review notes. The identity lifecycle is evidenced by the previous year's assessment. The encryption standard is documented alongside the ticket history for the period. The vulnerability queue is validated by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is checked against the most recent exercise record. The encryption standard is traced to the commissioning document. The hardened build is checked against the register of exceptions. Metrics are reported as trends rather than single data points.

The change process is compared with the ticket history for the period. The metric set is measured against the approved design baseline. The backup rotation is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

The vendor register is traced to the current written standard. The physical controls is reviewed against the ticket history for the period. The endpoint baseline is evidenced by the quarterly review notes. The change process is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The mobile standard is traced to the ticket history for the period. The retention schedule is checked against the current written standard. The threat model is measured against the current written standard. The vulnerability queue is reconciled with the agreed service level. Metrics are reported as trends rather than single data points.

The endpoint baseline is measured against the register of exceptions. The segmentation boundary is reviewed against the current written standard. Third parties must demonstrate the control before access is granted.

Each administrative account is traced to the evidence pack held by the owner. The risk register is validated by the signed exception log. The cloud baseline is measured against the signed exception log. Every internet-facing service is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

The patch calendar is checked against the register of exceptions. The access review process is measured against the register of exceptions. The classification scheme is evidenced by the signed exception log. The backup rotation is traced to the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is checked against the agreed service level. Every internet-facing service is traced to the commissioning document. The patch calendar is compared with the approved design baseline. The continuity plan is checked against the current written standard. Metrics are reported as trends rather than single data points.

The mobile standard is reconciled with the evidence pack held by the owner. The segmentation boundary is documented alongside the previous year's assessment. The mobile standard is documented alongside the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is documented alongside the current written standard. The classification scheme is reconciled with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The remote access path is traced to the approved design baseline. The retention schedule is evidenced by the dependency map. The monitoring pipeline is checked against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is checked against the ticket history for the period. Every internet-facing service is documented alongside the evidence pack held by the owner. The access review process is validated by the current written standard. The remote access path is checked against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The access review process is documented alongside the quarterly review notes. The remote access path is documented alongside the signed exception log. The control is tested at least once every twelve months.

The classification scheme is evidenced by the ticket history for the period. Every internet-facing service is documented alongside the approved design baseline. The vendor register is reconciled with the signed exception log. The segmentation boundary is traced to the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is documented alongside the quarterly review notes. The monitoring pipeline is measured against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is reviewed against the most recent exercise record. The vulnerability queue is reviewed against the signed exception log. The metric set is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is documented alongside the signed exception log. The access review process is compared with the agreed service level. The asset register is reviewed against the register of exceptions. The endpoint baseline is measured against the commissioning document. Metrics are reported as trends rather than single data points.

The physical controls is evidenced by the previous year's assessment. The privileged access list is reconciled with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is compared with the approved design baseline. The patch calendar is checked against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is measured against the commissioning document. The third-party register is reconciled with the evidence pack held by the owner. The physical controls is checked against the ticket history for the period. The retention schedule is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The change process is documented alongside the dependency map. The physical controls is validated by the ticket history for the period. The physical controls is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.

The awareness cycle is traced to the commissioning document. The third-party register is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The hardened build is checked against the agreed service level. The email authentication record is reviewed against the agreed service level. The metric set is measured against the previous year's assessment. The backup rotation is checked against the commissioning document. Metrics are reported as trends rather than single data points.

The threat model is reviewed against the quarterly review notes. The awareness cycle is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is checked against the ticket history for the period. The remote access path is reconciled with the register of exceptions. The cloud baseline is reconciled with the register of exceptions. The awareness cycle is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The metric set is reviewed against the dependency map. The awareness cycle is reconciled with the agreed service level. The endpoint baseline is traced to the signed exception log. The patch calendar is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The mobile standard is evidenced by the register of exceptions. Every internet-facing service is evidenced by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is compared with the approved design baseline. The vendor register is evidenced by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is checked against the approved design baseline. The metric set is documented alongside the register of exceptions. The backup rotation is checked against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The hardened build is reconciled with the signed exception log. The vulnerability queue is documented alongside the dependency map. The mobile standard is reviewed against the dependency map. The third-party register is documented alongside the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is reconciled with the previous year's assessment. The vulnerability queue is compared with the approved design baseline. The patch calendar is validated by the evidence pack held by the owner. The access review process is evidenced by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is reconciled with the previous year's assessment. The hardened build is reconciled with the evidence pack held by the owner. The classification scheme is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The hardened build is evidenced by the previous year's assessment. The change process is checked against the ticket history for the period. The segmentation boundary is validated by the agreed service level. The email authentication record is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

The classification scheme is reconciled with the agreed service level. The backup rotation is reviewed against the agreed service level. The physical controls is measured against the register of exceptions. Each administrative account is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is evidenced by the register of exceptions. The privileged access list is traced to the dependency map. The cloud baseline is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is traced to the approved design baseline. The metric set is traced to the previous year's assessment. The identity lifecycle is documented alongside the most recent exercise record. The classification scheme is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The vendor register is compared with the previous year's assessment. The privileged access list is checked against the register of exceptions. The continuity plan is reconciled with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vendor register is checked against the approved design baseline. The cloud baseline is traced to the signed exception log. The control is tested at least once every twelve months.

The metric set is validated by the register of exceptions. The continuity plan is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

The identity lifecycle is documented alongside the agreed service level. The retention schedule is compared with the most recent exercise record. The classification scheme is compared with the current written standard. Where automation is possible, the manual step is retained as a fallback.

The hardened build is validated by the register of exceptions. The classification scheme is compared with the ticket history for the period. The backup rotation is checked against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is evidenced by the ticket history for the period. The recovery test is checked against the agreed service level. The email authentication record is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

The metric set is checked against the most recent exercise record. The identity lifecycle is documented alongside the register of exceptions. Each administrative account is reconciled with the quarterly review notes. The remote access path is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

12. The identity lifecycle

The metric set is validated by the current written standard. The privileged access list is compared with the dependency map. Testing covers the failure case, not only the happy path.

The recovery test is documented alongside the current written standard. The change process is documented alongside the dependency map. The physical controls is compared with the previous year's assessment. The third-party register is traced to the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The retention schedule is documented alongside the ticket history for the period. The identity lifecycle is measured against the approved design baseline. The metric set is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is documented alongside the agreed service level. The vendor register is documented alongside the ticket history for the period. The threat model is compared with the current written standard. Testing covers the failure case, not only the happy path.

The asset register is compared with the current written standard. The encryption standard is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.