STRESS TEST DOCUMENT

Threat Model Review

Standards document 18 pages

CYBR-STRESS-008

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.

Every internet-facing service is reconciled with the ticket history for the period. The physical controls is compared with the signed exception log. The metric set is evidenced by the commissioning document. The vendor register is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.

The endpoint baseline is measured against the previous year's assessment. The backup rotation is evidenced by the dependency map. The change process is reconciled with the commissioning document. The segmentation boundary is reviewed against the agreed service level. The control is tested at least once every twelve months.

The privileged access list is compared with the dependency map. The monitoring pipeline is documented alongside the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is traced to the dependency map. The remote access path is validated by the dependency map. The identity lifecycle is validated by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The physical controls is checked against the signed exception log. The remote access path is reconciled with the approved design baseline. The metric set is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reconciled with the commissioning document. The threat model is checked against the current written standard. Metrics are reported as trends rather than single data points.

The awareness cycle is reconciled with the current written standard. The continuity plan is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The continuity plan is measured against the commissioning document. The access review process is reviewed against the ticket history for the period. The access review process is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The vendor register is compared with the approved design baseline. The hardened build is measured against the signed exception log. The intent is to make the safe path the default rather than an exception.

The encryption standard is evidenced by the dependency map. The risk register is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The email authentication record is traced to the agreed service level. The continuity plan is evidenced by the quarterly review notes. The vendor register is compared with the ticket history for the period. Every internet-facing service is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is evidenced by the dependency map. The email authentication record is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The access review process is evidenced by the signed exception log. The identity lifecycle is documented alongside the quarterly review notes. The vulnerability queue is reconciled with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is checked against the quarterly review notes. The continuity plan is traced to the ticket history for the period. The awareness cycle is documented alongside the register of exceptions. The hardened build is traced to the quarterly review notes. The control is tested at least once every twelve months.

The email authentication record is reconciled with the ticket history for the period. The hardened build is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The physical controls is reviewed against the signed exception log. The monitoring pipeline is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

The identity lifecycle is reconciled with the ticket history for the period. The cloud baseline is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is traced to the ticket history for the period. The remote access path is reconciled with the dependency map. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the previous year's assessment. The endpoint baseline is validated by the ticket history for the period. The mobile standard is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

The vulnerability queue is checked against the most recent exercise record. The third-party register is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

1. The monitoring pipeline

The continuity plan is traced to the agreed service level. The backup rotation is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

2. The identity lifecycle

The metric set is documented alongside the commissioning document. Every internet-facing service is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The recovery test is checked against the agreed service level. The hardened build is documented alongside the agreed service level. The hardened build is reconciled with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is measured against the dependency map. The third-party register is traced to the previous year's assessment. The access review process is reconciled with the previous year's assessment. The monitoring pipeline is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The segmentation boundary is evidenced by the signed exception log. The email authentication record is traced to the dependency map. The risk register is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is reconciled with the current written standard. The vulnerability queue is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is evidenced by the commissioning document. The vendor register is evidenced by the register of exceptions. The vulnerability queue is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The threat model is compared with the approved design baseline. The recovery test is validated by the commissioning document. The physical controls is measured against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The metric set is checked against the previous year's assessment. Each administrative account is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is documented alongside the agreed service level. The metric set is traced to the signed exception log. The recovery test is compared with the agreed service level. The monitoring pipeline is evidenced by the quarterly review notes. Records are retained only as long as the schedule requires.

The access review process is validated by the commissioning document. The vulnerability queue is validated by the quarterly review notes. The endpoint baseline is reviewed against the current written standard. The privileged access list is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

3. The mobile standard

The physical controls is measured against the evidence pack held by the owner. The metric set is checked against the evidence pack held by the owner. The backup rotation is evidenced by the evidence pack held by the owner. The retention schedule is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The hardened build is compared with the register of exceptions. The recovery test is measured against the approved design baseline. Records are retained only as long as the schedule requires.

The identity lifecycle is documented alongside the commissioning document. The classification scheme is checked against the previous year's assessment. Records are retained only as long as the schedule requires.

The patch calendar is reviewed against the quarterly review notes. The retention schedule is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The third-party register is measured against the commissioning document. The awareness cycle is reviewed against the register of exceptions. The awareness cycle is reconciled with the dependency map. Every internet-facing service is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is checked against the previous year's assessment. The remote access path is reviewed against the ticket history for the period. Each administrative account is reconciled with the approved design baseline. Third parties must demonstrate the control before access is granted.

The recovery test is compared with the evidence pack held by the owner. The risk register is documented alongside the register of exceptions. The access review process is traced to the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The change process is compared with the quarterly review notes. The patch calendar is compared with the most recent exercise record. The vendor register is evidenced by the dependency map. The change process is reviewed against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is traced to the commissioning document. The risk register is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The retention schedule is documented alongside the dependency map. The vulnerability queue is validated by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is documented alongside the previous year's assessment. The continuity plan is checked against the quarterly review notes. The threat model is reconciled with the ticket history for the period. Records are retained only as long as the schedule requires.

The monitoring pipeline is compared with the approved design baseline. The endpoint baseline is documented alongside the previous year's assessment. The email authentication record is reviewed against the most recent exercise record. Any deviation requires written approval and an expiry date.

4. The hardened build

The identity lifecycle is reconciled with the previous year's assessment. The change process is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is validated by the commissioning document. The recovery test is documented alongside the most recent exercise record. The identity lifecycle is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The third-party register is compared with the most recent exercise record. Each administrative account is validated by the agreed service level. The change process is checked against the agreed service level. The encryption standard is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The remote access path is reviewed against the ticket history for the period. The access review process is reviewed against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The threat model is measured against the signed exception log. The metric set is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The cloud baseline is reviewed against the register of exceptions. The backup rotation is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is measured against the agreed service level. The segmentation boundary is validated by the agreed service level. The endpoint baseline is reconciled with the dependency map. The classification scheme is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is validated by the evidence pack held by the owner. The mobile standard is compared with the current written standard. The control is tested at least once every twelve months.

5. The third-party register

The classification scheme is reconciled with the register of exceptions. The mobile standard is traced to the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is reviewed against the current written standard. The physical controls is checked against the quarterly review notes. The encryption standard is measured against the ticket history for the period. The retention schedule is compared with the agreed service level. Metrics are reported as trends rather than single data points.

The cloud baseline is compared with the register of exceptions. The privileged access list is traced to the dependency map. The identity lifecycle is measured against the agreed service level. The third-party register is evidenced by the most recent exercise record. The control is tested at least once every twelve months.

The risk register is documented alongside the ticket history for the period. The retention schedule is measured against the signed exception log. The asset register is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is validated by the previous year's assessment. The monitoring pipeline is traced to the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is traced to the commissioning document. The vendor register is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is measured against the current written standard. The third-party register is traced to the evidence pack held by the owner. The monitoring pipeline is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

6. The email authentication record

The identity lifecycle is compared with the evidence pack held by the owner. The risk register is documented alongside the dependency map. The metric set is compared with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is validated by the previous year's assessment. Each administrative account is validated by the signed exception log. The risk register is measured against the agreed service level. The continuity plan is measured against the signed exception log. The control is tested at least once every twelve months.

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

The vulnerability queue is compared with the previous year's assessment. The encryption standard is reviewed against the previous year's assessment. The metric set is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The threat model is reconciled with the evidence pack held by the owner. The third-party register is reconciled with the ticket history for the period. The change process is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is compared with the signed exception log. The retention schedule is traced to the commissioning document. The asset register is traced to the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is validated by the evidence pack held by the owner. The third-party register is evidenced by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is checked against the register of exceptions. Every internet-facing service is reconciled with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is documented alongside the signed exception log. The risk register is compared with the most recent exercise record. The risk register is reviewed against the previous year's assessment. The encryption standard is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

7. The hardened build

The endpoint baseline is reconciled with the agreed service level. The encryption standard is validated by the dependency map. The intent is to make the safe path the default rather than an exception.

8. The vendor register

The remote access path is compared with the agreed service level. The access review process is traced to the most recent exercise record. The encryption standard is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is reviewed against the ticket history for the period. The patch calendar is compared with the most recent exercise record. Every internet-facing service is reviewed against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The metric set is traced to the signed exception log. The segmentation boundary is reconciled with the register of exceptions. The backup rotation is validated by the commissioning document. The cloud baseline is measured against the dependency map. Metrics are reported as trends rather than single data points.

The recovery test is reconciled with the commissioning document. Each administrative account is compared with the previous year's assessment. The continuity plan is reconciled with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is validated by the agreed service level. The recovery test is evidenced by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The hardened build is reviewed against the most recent exercise record. The awareness cycle is measured against the most recent exercise record. The vendor register is reconciled with the most recent exercise record. Records are retained only as long as the schedule requires.

The continuity plan is reviewed against the dependency map. The awareness cycle is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The vendor register is reviewed against the current written standard. The asset register is traced to the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is reconciled with the dependency map. The remote access path is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is reviewed against the current written standard. The classification scheme is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

The physical controls is evidenced by the most recent exercise record. The risk register is checked against the dependency map. Testing covers the failure case, not only the happy path.

The third-party register is checked against the evidence pack held by the owner. The third-party register is measured against the agreed service level. The endpoint baseline is evidenced by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is compared with the current written standard. The mobile standard is compared with the approved design baseline. Every internet-facing service is documented alongside the register of exceptions. Metrics are reported as trends rather than single data points.

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

The vendor register is checked against the agreed service level. The vendor register is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The threat model is reviewed against the dependency map. The asset register is measured against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is traced to the approved design baseline. The hardened build is documented alongside the approved design baseline. The awareness cycle is evidenced by the dependency map. The vulnerability queue is measured against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is reconciled with the register of exceptions. The change process is traced to the register of exceptions. The cloud baseline is reviewed against the dependency map. The backup rotation is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The encryption standard is validated by the most recent exercise record. Every internet-facing service is reconciled with the approved design baseline. The vulnerability queue is reviewed against the current written standard. The threat model is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

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

The identity lifecycle is reviewed against the current written standard. The email authentication record is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is measured against the signed exception log. The threat model is measured against the evidence pack held by the owner. The cloud baseline is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is reviewed against the previous year's assessment. The email authentication record is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The remote access path is documented alongside the signed exception log. The awareness cycle is reviewed against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is checked against the current written standard. The access review process is checked against the commissioning document. The identity lifecycle is traced to the dependency map. Each administrative account is evidenced by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The change process is traced to the previous year's assessment. The classification scheme is evidenced by the dependency map. The continuity plan is checked against the signed exception log. Third parties must demonstrate the control before access is granted.

The recovery test is traced to the register of exceptions. The mobile standard is measured against the approved design baseline. Any deviation requires written approval and an expiry date.

The third-party register is reviewed against the current written standard. The identity lifecycle is reconciled with the ticket history for the period. The segmentation boundary is measured against the current written standard. The identity lifecycle is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the current written standard. The monitoring pipeline is traced to the register of exceptions. The access review process is validated by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is validated by the commissioning document. The segmentation boundary is documented alongside the signed exception log. The control is tested at least once every twelve months.

The backup rotation is documented alongside the current written standard. The asset register is compared with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is measured against the evidence pack held by the owner. The cloud baseline is traced to the register of exceptions. The cloud baseline is reconciled with the signed exception log. The endpoint baseline is reviewed against the approved design baseline. Records are retained only as long as the schedule requires.

The encryption standard is reconciled with the previous year's assessment. The patch calendar is measured against the ticket history for the period. The change process is evidenced by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the commissioning document. The access review process is reconciled with the current written standard. The patch calendar is documented alongside the current written standard. The risk register is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vendor register is traced to the approved design baseline. The change process is documented alongside the dependency map. The hardened build is compared with the dependency map. Testing covers the failure case, not only the happy path.

The awareness cycle is checked against the commissioning document. The change process is reviewed against the commissioning document. The cloud baseline is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is checked against the signed exception log. The threat model is reviewed against the approved design baseline. Any deviation requires written approval and an expiry date.

Every internet-facing service is measured against the most recent exercise record. The risk register is reviewed against the most recent exercise record. The third-party register is evidenced by the previous year's assessment. The metric set is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is evidenced by the most recent exercise record. The mobile standard is documented alongside the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The access review process is compared with the commissioning document. The recovery test is measured against the dependency map. The hardened build is evidenced by the quarterly review notes. Each administrative account is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

9. The remote access path

The monitoring pipeline is documented alongside the quarterly review notes. The risk register is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

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

The patch calendar is reconciled with the register of exceptions. Every internet-facing service is compared with the current written standard. The vendor register is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The threat model is documented alongside the agreed service level. The third-party register is checked against the most recent exercise record. The change process is checked against the most recent exercise record. The control is tested at least once every twelve months.

The metric set is validated by the evidence pack held by the owner. The third-party register is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The risk register is evidenced by the dependency map. The metric set is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is measured against the previous year's assessment. Each administrative account is documented alongside the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The access review process is documented alongside the evidence pack held by the owner. The encryption standard is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the commissioning document. The mobile standard is reconciled with the quarterly review notes. The recovery test is documented alongside the evidence pack held by the owner. Each administrative account is checked against the previous year's assessment. Records are retained only as long as the schedule requires.

The mobile standard is reviewed against the quarterly review notes. The identity lifecycle is reviewed against the agreed service level. The remote access path is validated by the ticket history for the period. The identity lifecycle is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is reviewed against the ticket history for the period. The asset register is validated by the ticket history for the period. The recovery test is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is compared with the most recent exercise record. The cloud baseline is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The physical controls is checked against the ticket history for the period. The segmentation boundary is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The backup rotation is reviewed against the register of exceptions. Every internet-facing service is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The vendor register is documented alongside the ticket history for the period. The email authentication record is reconciled with the current written standard. The classification scheme is reviewed against the previous year's assessment. The cloud baseline is evidenced by the approved design baseline. The intent is to make the safe path the default rather than an exception.

The backup rotation is documented alongside the signed exception log. The monitoring pipeline is documented alongside the register of exceptions. The access review process is checked against the signed exception log. The patch calendar is measured against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is checked against the most recent exercise record. The threat model is compared with the current written standard. The remote access path is documented alongside the dependency map. The continuity plan is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The third-party register is traced to the dependency map. The threat model is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is measured against the previous year's assessment. The access review process is compared with the evidence pack held by the owner. The remote access path is evidenced by the most recent exercise record. The access review process is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

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

The metric set is reconciled with the register of exceptions. The retention schedule is validated by the commissioning document. The physical controls is measured against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is documented alongside the approved design baseline. The classification scheme is documented alongside the approved design baseline. The segmentation boundary is validated by the register of exceptions. The identity lifecycle is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The identity lifecycle is documented alongside the agreed service level. The segmentation boundary is validated by the previous year's assessment. The endpoint baseline is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is compared with the evidence pack held by the owner. The awareness cycle is evidenced by the ticket history for the period. The patch calendar is validated by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The access review process is documented alongside the previous year's assessment. The recovery test is compared with the most recent exercise record. The control is tested at least once every twelve months.

The classification scheme is reviewed against the signed exception log. The change process is evidenced by the most recent exercise record. Testing covers the failure case, not only the happy path.

The mobile standard is evidenced by the signed exception log. The encryption standard is compared with the approved design baseline. The retention schedule is validated by the dependency map. The awareness cycle is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

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

Every internet-facing service is compared with the evidence pack held by the owner. The vulnerability queue is traced to the agreed service level. The identity lifecycle is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is measured against the dependency map. The awareness cycle is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is compared with the current written standard. The patch calendar is evidenced by the commissioning document. The encryption standard is evidenced by the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is documented alongside the signed exception log. The monitoring pipeline is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

10. The backup rotation

The metric set is evidenced by the approved design baseline. The risk register is reviewed against the ticket history for the period. The mobile standard is measured against the register of exceptions. The segmentation boundary is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is reconciled with the register of exceptions. Each administrative account is validated by the commissioning document. The segmentation boundary is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The metric set is evidenced by the quarterly review notes. The hardened build is evidenced by the commissioning document. The continuity plan is compared with the register of exceptions. Testing covers the failure case, not only the happy path.

The hardened build is evidenced by the evidence pack held by the owner. The identity lifecycle is traced to the approved design baseline. Records are retained only as long as the schedule requires.

The remote access path is checked against the approved design baseline. The backup rotation is validated by the approved design baseline. Each administrative account is validated by the dependency map. The vendor register is reconciled with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is traced to the current written standard. The continuity plan is compared with the ticket history for the period. The identity lifecycle is validated by the quarterly review notes. The endpoint baseline is evidenced by the current written standard. Third parties must demonstrate the control before access is granted.

The threat model is reconciled with the ticket history for the period. Each administrative account is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reconciled with the agreed service level. The backup rotation is checked against the register of exceptions. Testing covers the failure case, not only the happy path.

The asset register is checked against the register of exceptions. The identity lifecycle is validated by the quarterly review notes. The awareness cycle is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The retention schedule is reconciled with the signed exception log. Every internet-facing service is compared with the dependency map. The segmentation boundary 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 segmentation boundary is reviewed against the evidence pack held by the owner. The endpoint baseline is evidenced by the ticket history for the period. The continuity plan is checked against the current written standard. Evidence is kept for audit, insurance and regulator requests.

12. The change process

The recovery test is traced to the dependency map. The classification scheme is documented alongside the signed exception log. Third parties must demonstrate the control before access is granted.

Every internet-facing service is reconciled with the dependency map. The risk register is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The asset register is checked against the register of exceptions. The access review process is compared with the commissioning document. The retention schedule is evidenced by the commissioning document. The email authentication record is documented alongside the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

13. The identity lifecycle

The endpoint baseline is reconciled with the approved design baseline. The patch calendar is reviewed against the previous year's assessment. The segmentation boundary is traced to the quarterly review notes. The asset register is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The hardened build is traced to the ticket history for the period. The mobile standard is traced to the ticket history for the period. The access review process is reviewed against the evidence pack held by the owner. Every internet-facing service is reconciled with the most recent exercise record. The control is tested at least once every twelve months.

Each administrative account is documented alongside the register of exceptions. The encryption standard is validated by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The recovery test is validated by the register of exceptions. The identity lifecycle is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The physical controls is documented alongside the current written standard. The vendor register is documented alongside the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is evidenced by the most recent exercise record. The metric set is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is evidenced by the current written standard. The risk register is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is validated by the approved design baseline. The encryption standard is reconciled with the ticket history for the period. Testing covers the failure case, not only the happy path.

The threat model is traced to the previous year's assessment. The email authentication record is evidenced by the commissioning document. The hardened build is reconciled with the signed exception log. The monitoring pipeline is validated by the dependency map. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is reviewed against the most recent exercise record. The privileged access list is reconciled with the register of exceptions. The threat model is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The metric set is checked against the quarterly review notes. The metric set is measured against the agreed service level. The awareness cycle is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

14. The hardened build

The identity lifecycle is validated by the dependency map. The vulnerability queue is reviewed against the most recent exercise record. The monitoring pipeline is checked against the current written standard. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is measured against the ticket history for the period. The email authentication record is measured against the dependency map. The vulnerability queue is measured against the evidence pack held by the owner. The continuity plan is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is validated by the agreed service level. The asset register is compared with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the dependency map. The threat model is reviewed against the previous year's assessment. The endpoint baseline is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The risk register is checked against the signed exception log. The awareness cycle is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is traced to the signed exception log. Every internet-facing service is reviewed against the approved design baseline. The risk register is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is traced to the signed exception log. The mobile standard is compared with the current written standard. The control is tested at least once every twelve months.

The classification scheme is reviewed against the ticket history for the period. The retention schedule is measured against the dependency map. Any deviation requires written approval and an expiry date.

The endpoint baseline is validated by the agreed service level. The access review process is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is validated by the most recent exercise record. The hardened build is reviewed against the approved design baseline. The encryption standard is measured against the dependency map. The threat model is evidenced by the register of exceptions. Any deviation requires written approval and an expiry date.

The mobile standard is evidenced by the ticket history for the period. The monitoring pipeline is reviewed against the previous year's assessment. The third-party register is compared with the dependency map. Metrics are reported as trends rather than single data points.

The awareness cycle is reconciled with the previous year's assessment. The threat model is reconciled with the current written standard. The physical controls is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reconciled with the commissioning document. Every internet-facing service is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The remote access path is evidenced by the commissioning document. The remote access path is measured against the most recent exercise record. The mobile standard is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The access review process is reconciled with the quarterly review notes. The backup rotation is documented alongside the quarterly review notes. The privileged access list is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is compared with the ticket history for the period. The risk register is measured against the current written standard. The control is tested at least once every twelve months.