Logging and Monitoring Baseline

Benchmark document 18 pages

CYBR-STRESS-040

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

The remote access path is reviewed against the register of exceptions. The threat model is checked against the quarterly review notes. The threat model is traced to the approved design baseline. The physical controls is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The change process is measured against the current written standard. The recovery test is checked against the dependency map. The monitoring pipeline is reconciled with the approved design baseline. The physical controls is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is documented alongside the current written standard. The vendor register is reconciled with the quarterly review notes. The risk register is reconciled with the quarterly review notes. The physical controls is documented alongside the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is evidenced by the current written standard. The continuity plan is evidenced by the register of exceptions. Each administrative account is evidenced by the dependency map. Metrics are reported as trends rather than single data points.

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

The physical controls is compared with the quarterly review notes. The recovery test is traced to the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is evidenced by the register of exceptions. The mobile standard is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The asset register is evidenced by the current written standard. The awareness cycle is checked against the agreed service level. The segmentation boundary is reviewed against the most recent exercise record. The third-party register is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is reviewed against the previous year's assessment. The physical controls is reviewed against the evidence pack held by the owner. The metric set is measured against the signed exception log. The remote access path is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is documented alongside the quarterly review notes. The monitoring pipeline is traced to the signed exception log. The vulnerability queue is checked against the approved design baseline. The mobile standard is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The threat model is measured against the approved design baseline. The physical controls is documented alongside the previous year's assessment. The identity lifecycle is evidenced by the current written standard. Third parties must demonstrate the control before access is granted.

The metric set is compared with the quarterly review notes. The metric set is reviewed against the agreed service level. Records are retained only as long as the schedule requires.

The awareness cycle is documented alongside the agreed service level. The vendor register is traced to the signed exception log. The vulnerability queue is compared with the approved design baseline. Every internet-facing service is documented alongside the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The asset register is reconciled with the current written standard. The monitoring pipeline is validated by the approved design baseline. The cloud baseline is traced to the register of exceptions. The continuity plan is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is traced to the signed exception log. The vendor register is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

The segmentation boundary is traced to the signed exception log. The awareness cycle is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The remote access path is validated by the previous year's assessment. The physical controls is measured against the signed exception log. The threat model is traced to the dependency map. The continuity plan is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is traced to the quarterly review notes. Every internet-facing service is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is reconciled with the ticket history for the period. The access review process is reviewed against the commissioning document. The change process is traced to the approved design baseline. Records are retained only as long as the schedule requires.

The change process is reconciled with the commissioning document. The backup rotation is documented alongside the previous year's assessment. The encryption standard is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is validated by the current written standard. The risk register is reviewed against the current written standard. The third-party register is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

1. The metric set

The threat model is traced to the agreed service level. The threat model is measured against the ticket history for the period. The physical controls is reconciled with the approved design baseline. Third parties must demonstrate the control before access is granted.

The hardened build is validated by the quarterly review notes. The recovery test is reconciled with the approved design baseline. Third parties must demonstrate the control before access is granted.

The encryption standard is compared with the previous year's assessment. The patch calendar is checked against the quarterly review notes. Every internet-facing service is traced to the evidence pack held by the owner. The vulnerability queue is evidenced by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The recovery test is compared with the dependency map. The email authentication record is evidenced by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is checked against the commissioning document. The risk register is reconciled with the most recent exercise record. The segmentation boundary is checked against the agreed service level. The vulnerability queue is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The risk register is reviewed against the dependency map. The endpoint baseline is validated by the ticket history for the period. The awareness cycle is documented alongside the commissioning document. The continuity plan is reviewed against the most recent exercise record. Third parties must demonstrate the control before access is granted.

Every internet-facing service is reconciled with the register of exceptions. The privileged access list is checked against the signed exception log. Metrics are reported as trends rather than single data points.

The asset register is documented alongside the current written standard. The access review process is reconciled with the agreed service level. The vendor register is checked against the agreed service level. Each administrative account is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The asset register is evidenced by the approved design baseline. The endpoint baseline is traced to the dependency map. The monitoring pipeline is traced to the current written standard. The physical controls is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

2. Each administrative account

The identity lifecycle is validated by the approved design baseline. The mobile standard is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The metric set is validated by the evidence pack held by the owner. The vendor register is traced to the evidence pack held by the owner. The endpoint baseline is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

3. The third-party register

The threat model is validated by the signed exception log. The hardened build is reconciled with the signed exception log. The patch calendar is documented alongside the ticket history for the period. The threat model is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The risk register is measured against the evidence pack held by the owner. The physical controls is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The mobile standard is reviewed against the register of exceptions. The recovery test is validated by the most recent exercise record. The vendor register is validated by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is measured against the ticket history for the period. The privileged access list is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is documented alongside the evidence pack held by the owner. The third-party register is measured against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is measured against the dependency map. The remote access path is checked against the previous year's assessment. The patch calendar is measured against the quarterly review notes. The continuity plan is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The classification scheme is compared with the current written standard. The continuity plan is traced to the ticket history for the period. The continuity plan is traced to the signed exception log. Records are retained only as long as the schedule requires.

The access review process is reconciled with the dependency map. The monitoring pipeline is traced to the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The metric set is reviewed against the approved design baseline. The classification scheme is checked against the approved design baseline. The control is tested at least once every twelve months.

The hardened build is checked against the most recent exercise record. The patch calendar is compared with the previous year's assessment. The classification scheme is checked against the approved design baseline. The threat model is reviewed against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is checked against the signed exception log. Each administrative account is checked against the commissioning document. The metric set is validated by the approved design baseline. The threat model is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is documented alongside the dependency map. The change process is traced to the ticket history for the period. The privileged access list is reconciled with the most recent exercise record. The threat model is validated by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

4. The remote access path

The email authentication record is reviewed against the quarterly review notes. Every internet-facing service is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The access review process is documented alongside the agreed service level. The vendor register is validated by the register of exceptions. Each administrative account is measured against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The mobile standard is reviewed against the signed exception log. The backup rotation is reconciled with the quarterly review notes. The hardened build is reconciled with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The third-party register is validated by the approved design baseline. The monitoring pipeline is documented alongside the evidence pack held by the owner. The awareness cycle is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

5. The metric set

The endpoint baseline is compared with the signed exception log. The third-party register is traced to the evidence pack held by the owner. The patch calendar is validated by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is measured against the commissioning document. The change process is measured against the signed exception log. The cloud baseline is evidenced by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The metric set is measured against the quarterly review notes. The continuity plan is reconciled with the agreed service level. The remote access path is checked against the register of exceptions. The email authentication record is documented alongside the evidence pack held by the owner. The control is tested at least once every twelve months.

The recovery test is measured against the most recent exercise record. The privileged access list is measured against the quarterly review notes. The control is tested at least once every twelve months.

The metric set is checked against the quarterly review notes. The metric set is evidenced by the approved design baseline. The identity lifecycle is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

The recovery test is documented alongside the signed exception log. The remote access path is reviewed against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

6. The patch calendar

The remote access path is measured against the signed exception log. The mobile standard is measured against the most recent exercise record. The recovery test is reconciled with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The asset register is compared with the evidence pack held by the owner. The continuity plan is reconciled with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is traced to the previous year's assessment. The encryption standard is validated by the signed exception log. The access review process is reviewed against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is evidenced by the approved design baseline. The remote access path is validated by the evidence pack held by the owner. The physical controls is compared with the ticket history for the period. Third parties must demonstrate the control before access is granted.

Every internet-facing service is traced to the evidence pack held by the owner. The vulnerability queue is traced to the evidence pack held by the owner. The email authentication record is compared with the commissioning document. The asset register is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is compared with the quarterly review notes. The remote access path is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the dependency map. The access review process is reviewed against the commissioning document. The recovery test is validated by the commissioning document. The awareness cycle is documented alongside the commissioning document. Third parties must demonstrate the control before access is granted.

The vulnerability queue is documented alongside the dependency map. The segmentation boundary is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is traced to the previous year's assessment. The encryption standard is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The metric set is compared with the previous year's assessment. The physical controls is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The change process is reconciled with the commissioning document. The vendor register is compared with the agreed service level. The monitoring pipeline is traced to the quarterly review notes. The monitoring pipeline is evidenced by the dependency map. Any deviation requires written approval and an expiry date.

Every internet-facing service is checked against the quarterly review notes. The backup rotation is evidenced by the previous year's assessment. The encryption standard is documented alongside the previous year's assessment. The segmentation boundary is evidenced by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is documented alongside the most recent exercise record. The continuity plan is reconciled with the most recent exercise record. The vendor register is validated by the signed exception log. The remote access path is documented alongside the agreed service level. Metrics are reported as trends rather than single data points.

Each administrative account is validated by the ticket history for the period. The monitoring pipeline is checked against the approved design baseline. The asset register is documented alongside the agreed service level. The recovery test is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The change process is evidenced by the quarterly review notes. The recovery test is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

The identity lifecycle is reconciled with the register of exceptions. The segmentation boundary is validated by the commissioning document. Every internet-facing service is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The retention schedule is measured against the evidence pack held by the owner. The patch calendar is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

8. The vendor register

Each administrative account is reviewed against the dependency map. The threat model is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The access review process is traced to the evidence pack held by the owner. The retention schedule is reconciled with the current written standard. The cloud baseline is compared with the most recent exercise record. The physical controls is reconciled with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is reviewed against the previous year's assessment. The risk register is traced to the dependency map. The segmentation boundary is traced to the register of exceptions. The metric set is documented alongside the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Test result attached to the record.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Owner named and recorded in the register.

Every internet-facing service is traced to the approved design baseline. Every internet-facing service is documented alongside the most recent exercise record. The access review process is evidenced by the agreed service level. Every internet-facing service is reconciled with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The risk register is documented alongside the ticket history for the period. The third-party register is reviewed against the current written standard. The vendor register is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is traced to the agreed service level. The remote access path is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is measured against the current written standard. The risk register is documented alongside the evidence pack held by the owner. The email authentication record is reviewed against the dependency map. The threat model is reconciled with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is checked against the register of exceptions. The cloud baseline is documented alongside the dependency map. The identity lifecycle is documented alongside the dependency map. The vulnerability queue is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The risk register is reviewed against the register of exceptions. The vulnerability queue is reconciled with the register of exceptions. The identity lifecycle is measured against the dependency map. The access review process is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The metric set is reviewed against the quarterly review notes. The endpoint baseline is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

10. The vendor register

The retention schedule is compared with the quarterly review notes. The cloud baseline is measured against the approved design baseline. Any deviation requires written approval and an expiry date.

The asset register is reviewed against the quarterly review notes. The access review process is checked against the previous year's assessment. The awareness cycle is evidenced by the signed exception log. The access review process is measured against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is evidenced by the agreed service level. The segmentation boundary is reconciled with the commissioning document. The third-party register is compared with the commissioning document. The hardened build is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The recovery test is evidenced by the commissioning document. The patch calendar is reconciled with the evidence pack held by the owner. The access review process is evidenced by the approved design baseline. The vendor register is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The identity lifecycle is checked against the evidence pack held by the owner. The endpoint baseline is evidenced by the approved design baseline. The vendor register is documented alongside the signed exception log. The classification scheme is reviewed against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is checked against the approved design baseline. The risk register is documented alongside the quarterly review notes. The backup rotation is traced to the most recent exercise record. The classification scheme is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

Every internet-facing service is traced to the current written standard. The vulnerability queue is documented alongside the agreed service level. The threat model is documented alongside the commissioning document. The awareness cycle is compared with the agreed service level. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is validated by the quarterly review notes. The identity lifecycle is compared with the current written standard. The vendor register is traced to the current written standard. The remote access path is compared with the agreed service level. The control is tested at least once every twelve months.

The endpoint baseline is reviewed against the commissioning document. The metric set is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is validated by the most recent exercise record. The vendor register is evidenced by the current written standard. The risk register is validated by the quarterly review notes. The access review process is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

11. The vendor register

The asset register is validated by the dependency map. The encryption standard is checked against the register of exceptions. The vendor register is measured against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The threat model is validated by the previous year's assessment. The recovery test is measured against the previous year's assessment. The control is tested at least once every twelve months.

The classification scheme is reconciled with the dependency map. The third-party register is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

The threat model is validated by the quarterly review notes. The backup rotation is traced to the evidence pack held by the owner. The backup rotation is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

The threat model is traced to the signed exception log. The asset register is evidenced by the register of exceptions. The control is tested at least once every twelve months.

12. The continuity plan

The asset register is reconciled with the dependency map. The patch calendar is validated by the ticket history for the period. The physical controls is validated by the agreed service level. Every internet-facing service is traced to the current written standard. Third parties must demonstrate the control before access is granted.

The access review process is traced to the signed exception log. The third-party register is traced to the agreed service level. The asset register is compared with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is documented alongside the commissioning document. The email authentication record is documented alongside the evidence pack held by the owner. The mobile standard is measured against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The vendor register is compared with the signed exception log. The patch calendar is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is measured against the current written standard. The retention schedule is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The mobile standard is traced to the approved design baseline. The risk register is compared with the agreed service level. The asset register is documented alongside the most recent exercise record. The privileged access list is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is checked against the most recent exercise record. The privileged access list is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

Each administrative account is checked against the quarterly review notes. The physical controls is reconciled with the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Test result attached to the record.

Each administrative account is checked against the signed exception log. The privileged access list is evidenced by the current written standard. The hardened build is compared with the agreed service level. The physical controls is compared with the current written standard. Third parties must demonstrate the control before access is granted.

The vulnerability queue is reviewed against the commissioning document. The privileged access list is traced to the dependency map. The encryption standard is reviewed against the previous year's assessment. The third-party register is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The vendor register is reconciled with the most recent exercise record. The cloud baseline is reviewed against the ticket history for the period. The privileged access list is documented alongside the most recent exercise record. The third-party register is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is measured against the most recent exercise record. The awareness cycle is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The access review process is evidenced by the quarterly review notes. The threat model is reconciled with the signed exception log. The continuity plan is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

Every internet-facing service is traced to the dependency map. Every internet-facing service is reconciled with the evidence pack held by the owner. The mobile standard is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is documented alongside the signed exception log. The threat model is reconciled with the current written standard. Evidence is kept for audit, insurance and regulator requests.

- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The metric set is traced to the commissioning document. The third-party register is documented alongside the most recent exercise record. The classification scheme is traced to the agreed service level. The endpoint baseline is documented alongside the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is reviewed against the ticket history for the period. The awareness cycle is measured against the agreed service level. The physical controls is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The physical controls is documented alongside the current written standard. The hardened build is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is reviewed against the evidence pack held by the owner. The patch calendar is reviewed against the signed exception log. Records are retained only as long as the schedule requires.

The metric set is traced to the quarterly review notes. The backup rotation is reviewed against the previous year's assessment. The patch calendar is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The identity lifecycle is evidenced by the register of exceptions. The continuity plan is validated by the register of exceptions. The cloud baseline is documented alongside the evidence pack held by the owner. The threat model is reviewed against the quarterly review notes. Any deviation requires written approval and an expiry date.

Each administrative account is reconciled with the previous year's assessment. The email authentication record is evidenced by the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is reconciled with the ticket history for the period. The email authentication record is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The endpoint baseline is documented alongside the evidence pack held by the owner. Each administrative account is measured against the most recent exercise record. Each administrative account is compared with the signed exception log. The monitoring pipeline is documented alongside the agreed service level. Any deviation requires written approval and an expiry date.

The access review process is measured against the quarterly review notes. The hardened build is validated by the signed exception log. The retention schedule is traced to the ticket history for the period. The threat model is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

The identity lifecycle is validated by the previous year's assessment. The vendor register is reviewed against the most recent exercise record. The monitoring pipeline is checked against the commissioning document. Metrics are reported as trends rather than single data points.

Every internet-facing service is checked against the evidence pack held by the owner. The patch calendar is compared with the approved design baseline. Every internet-facing service is evidenced by the current written standard. The patch calendar is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

The metric set is compared with the most recent exercise record. The cloud baseline is evidenced by the current written standard. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reviewed against the commissioning document. The change process is documented alongside the most recent exercise record. Each administrative account is reviewed against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is measured against the dependency map. The monitoring pipeline is validated by the dependency map. The change process is validated by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The vulnerability queue is reviewed against the dependency map. The mobile standard is compared with the ticket history for the period. Each administrative account is evidenced by the most recent exercise record. The patch calendar is evidenced by the approved design baseline. Testing covers the failure case, not only the happy path.

The classification scheme is measured against the previous year's assessment. The hardened build is documented alongside the agreed service level. The cloud baseline is compared with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is traced to the most recent exercise record. The email authentication record is traced to the dependency map. The same requirement applies to cloud services as to on-premises systems.

The metric set is checked against the approved design baseline. The change process is traced to the previous year's assessment. Each administrative account is checked against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is documented alongside the quarterly review notes. The backup rotation is reviewed against the commissioning document. The asset register is compared with the signed exception log. The asset register is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The recovery test is checked against the most recent exercise record. The remote access path is checked against the most recent exercise record. The change process is checked against the most recent exercise record. The mobile standard is validated by the commissioning document. Records are retained only as long as the schedule requires.

The patch calendar is compared with the register of exceptions. The awareness cycle is checked against the register of exceptions. Any deviation requires written approval and an expiry date.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Backup of the change retained for rollback.

The asset register is measured against the most recent exercise record. The patch calendar is checked against the current written standard. The classification scheme is compared with the signed exception log. The retention schedule is measured against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is evidenced by the approved design baseline. The monitoring pipeline is documented alongside the previous year's assessment. The retention schedule is traced to the evidence pack held by the owner. The physical controls is reconciled with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is compared with the most recent exercise record. The email authentication record is evidenced by the ticket history for the period. The identity lifecycle is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is evidenced by the most recent exercise record. The recovery test is documented alongside the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is reviewed against the approved design baseline. The endpoint baseline is documented alongside the commissioning document. The threat model is traced to the current written standard. The physical controls is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

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

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Escalation path agreed with the service owner.

The patch calendar is reconciled with the quarterly review notes. Every internet-facing service is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

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

The physical controls is compared with the register of exceptions. The backup rotation is measured against the current written standard. The monitoring pipeline is traced to the quarterly review notes. Third parties must demonstrate the control before access is granted.

The metric set is documented alongside the dependency map. The privileged access list is compared with the dependency map. The awareness cycle is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The asset register is evidenced by the dependency map. The vulnerability queue is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is traced to the current written standard. The segmentation boundary is reviewed against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is documented alongside the evidence pack held by the owner. The access review process is documented alongside the register of exceptions. The physical controls is evidenced by the ticket history for the period. The email authentication record is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is documented alongside the current written standard. The endpoint baseline is reconciled with the ticket history for the period. The monitoring pipeline is documented alongside the agreed service level. The backup rotation is traced to the dependency map. Records are retained only as long as the schedule requires.

The monitoring pipeline is traced to the previous year's assessment. The change process is traced to the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is checked against the quarterly review notes. The remote access path is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is reconciled with the previous year's assessment. The physical controls is reviewed against the quarterly review notes. The mobile standard is evidenced by the current written standard. The monitoring pipeline is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is validated by the current written standard. The identity lifecycle is evidenced by the dependency map. The identity lifecycle is reconciled with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is validated by the approved design baseline. The identity lifecycle is reconciled with the dependency map. The segmentation boundary is reconciled with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The metric set is reviewed against the evidence pack held by the owner. The physical controls is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is measured against the current written standard. The threat model is traced to the ticket history for the period. The hardened build is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

The vulnerability queue is evidenced by the previous year's assessment. The continuity plan is compared with the ticket history for the period. The cloud baseline is checked against the current written standard. Every internet-facing service is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

The retention schedule is validated by the dependency map. The endpoint baseline is reviewed against the most recent exercise record. The mobile standard is evidenced by the previous year's assessment. The patch calendar is validated by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The vendor register is validated by the most recent exercise record. The hardened build is documented alongside the agreed service level. Third parties must demonstrate the control before access is granted.

The third-party register is traced to the most recent exercise record. The identity lifecycle is measured against the most recent exercise record. The threat model is documented alongside the register of exceptions. The retention schedule is evidenced by the previous year's assessment. Any deviation requires written approval and an expiry date.

- Review date scheduled and visible.
- Test result attached to the record.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.

The email authentication record is validated by the current written standard. The backup rotation is reconciled with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The metric set is documented alongside the agreed service level. Each administrative account is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The physical controls is checked against the quarterly review notes. The risk register is reconciled with the previous year's assessment. The access review process is evidenced by the quarterly review notes. Each administrative account is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.