Cloud Configuration Standard

Standards document 18 pages

CYBR-STRESS-078

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 mobile standard is reconciled with the most recent exercise record. The awareness cycle is validated by the previous year's assessment. The segmentation boundary is traced to the dependency map. Every internet-facing service is checked against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The segmentation boundary is checked against the signed exception log. The classification scheme is evidenced by the signed exception log. The access review process is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The recovery test is checked against the evidence pack held by the owner. The asset register is reconciled with the approved design baseline. Every internet-facing service is checked against the ticket history for the period. The backup rotation is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The patch calendar is validated by the previous year's assessment. The vulnerability queue is traced to the signed exception log. Any deviation requires written approval and an expiry date.

Every internet-facing service is validated by the commissioning document. The hardened build is documented alongside the evidence pack held by the owner. The third-party register is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The risk register is measured against the evidence pack held by the owner. The patch calendar is documented alongside the previous year's assessment. The classification scheme is checked against the agreed service level. The awareness cycle is traced to the most recent exercise record. Third parties must demonstrate the control before access is granted.

The identity lifecycle is documented alongside the current written standard. The retention schedule is compared with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is reconciled with the current written standard. The third-party register is measured against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is checked against the most recent exercise record. The change process is documented alongside the commissioning document. Each administrative account is documented alongside the evidence pack held by the owner. The threat model is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The mobile standard is measured against the agreed service level. The continuity plan is measured against the current written standard. The monitoring pipeline is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The threat model is compared with the signed exception log. The metric set is validated by the ticket history for the period. The metric set is measured against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The asset register is validated by the quarterly review notes. Each administrative account is documented alongside the quarterly review notes. The segmentation boundary is measured against the ticket history for the period. The access review process is traced to the ticket history for the period. Metrics are reported as trends rather than single data points.

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

The recovery test is reconciled with the evidence pack held by the owner. The retention schedule is checked against the dependency map. The threat model is measured against the approved design baseline. Any deviation requires written approval and an expiry date.

The remote access path is reviewed against the quarterly review notes. The risk register is evidenced by the dependency map. The remote access path is compared with the commissioning document. The retention schedule is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is traced to the commissioning document. Each administrative account is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The physical controls is measured against the current written standard. The identity lifecycle is traced to the current written standard. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the evidence pack held by the owner. The physical controls is compared with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

2. The hardened build

The classification scheme is reconciled with the quarterly review notes. The privileged access list is documented alongside the agreed service level. The change process is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is validated by the approved design baseline. The change process is checked against the signed exception log. The vulnerability queue is compared with the approved design baseline. Every internet-facing service is traced to the signed exception log. Metrics are reported as trends rather than single data points.

The vendor register is traced to the previous year's assessment. The threat model is reconciled with the evidence pack held by the owner. The risk register is validated by the dependency map. The remote access path is documented alongside the dependency map. Records are retained only as long as the schedule requires.

The cloud baseline is traced to the commissioning document. The backup rotation is documented alongside the register of exceptions. The endpoint baseline is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is validated by the ticket history for the period. Every internet-facing service is reconciled with the dependency map. The metric set is checked against the current written standard. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is documented alongside the signed exception log. The vulnerability queue is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

Every internet-facing service is compared with the register of exceptions. The access review process is reconciled with the approved design baseline. The third-party register is traced to the dependency map. Metrics are reported as trends rather than single data points.

The patch calendar is reconciled with the most recent exercise record. The awareness cycle is checked against the commissioning document. Metrics are reported as trends rather than single data points.

The vendor register is reviewed against the register of exceptions. The identity lifecycle is reconciled with the most recent exercise record. Each administrative account is checked against the previous year's assessment. Each administrative account is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The hardened build is traced to the ticket history for the period. The segmentation boundary is measured against the quarterly review notes. The asset register is documented alongside the dependency map. The metric set is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

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

The identity lifecycle is compared with the approved design baseline. The patch calendar is measured against the commissioning document. Every internet-facing service is traced to the ticket history for the period. The vendor register is measured against the dependency map. Any deviation requires written approval and an expiry date.

The remote access path is reviewed against the current written standard. The monitoring pipeline is compared with the previous year's assessment. The endpoint baseline is evidenced by the register of exceptions. The mobile standard is evidenced by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is traced to the quarterly review notes. The vendor register is documented alongside the approved design baseline. The asset register is traced to the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is traced to the quarterly review notes. The continuity plan is reconciled with the evidence pack held by the owner. The encryption standard is checked against the previous year's assessment. The continuity plan is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is reviewed against the previous year's assessment. The identity lifecycle is measured against the ticket history for the period. The third-party register is traced to the quarterly review notes. The classification scheme is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

The continuity plan is documented alongside the commissioning document. The endpoint baseline is measured against the signed exception log. The continuity plan is traced to the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is validated by the evidence pack held by the owner. The patch calendar is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The risk register is validated by the most recent exercise record. The monitoring pipeline is reviewed against the register of exceptions. The cloud baseline is checked against the signed exception log. The vendor register is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

The email authentication record is documented alongside the dependency map. 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.

The hardened build is validated by the quarterly review notes. The segmentation boundary is reconciled with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is reviewed against the signed exception log. The remote access path is checked against the register of exceptions. The endpoint baseline is documented alongside the dependency map. The recovery test is documented alongside the register of exceptions. Records are retained only as long as the schedule requires.

The access review process is validated by the signed exception log. The hardened build is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is measured against the approved design baseline. The recovery test is reconciled with the ticket history for the period. The asset register is checked against the ticket history for the period. The control is tested at least once every twelve months.

3. The awareness cycle

The hardened build is validated by the previous year's assessment. The hardened build is evidenced by the register of exceptions. The patch calendar is compared with the commissioning document. The access review process is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is evidenced by the evidence pack held by the owner. The asset register is checked against the agreed service level. Testing covers the failure case, not only the happy path.

The physical controls is reconciled with the quarterly review notes. The cloud baseline is reconciled with the commissioning document. The backup rotation is measured against the register of exceptions. The recovery test is reviewed against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The threat model is evidenced by the commissioning document. The vendor register is checked against the commissioning document. Testing covers the failure case, not only the happy path.

The third-party register is documented alongside the current written standard. The retention schedule is evidenced by the quarterly review notes. The change process is evidenced by the current written standard. The risk register is measured against the quarterly review notes. Records are retained only as long as the schedule requires.

The asset register is measured against the evidence pack held by the owner. The metric set is checked against the quarterly review notes. The identity lifecycle is documented alongside the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is compared with the evidence pack held by the owner. Every internet-facing service is compared with the previous year's assessment. The encryption standard is documented alongside the register of exceptions. The risk register is measured against the ticket history for the period. The control is tested at least once every twelve months.

The change process is measured against the previous year's assessment. The email authentication record is documented alongside the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The risk register is checked against the quarterly review notes. The access review process is traced to the previous year's assessment. The cloud baseline is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reviewed against the current written standard. The hardened build is reviewed against the commissioning document. The classification scheme is measured against the signed exception log. The recovery test is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The metric set is measured against the ticket history for the period. The asset register is checked against the current written standard. Every internet-facing service is evidenced by the agreed service level. The control is tested at least once every twelve months.

The vulnerability queue is measured against the ticket history for the period. The asset register is checked against the dependency map. Every internet-facing service is compared with the signed exception log. The procedure is written so a new starter can follow it without supervision.

The hardened build is reviewed against the agreed service level. The monitoring pipeline is reconciled with the previous year's assessment. Every internet-facing service is reviewed against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is reconciled with the signed exception log. The vendor register is checked against the ticket history for the period. Testing covers the failure case, not only the happy path.

The classification scheme is checked against the register of exceptions. The vulnerability queue is measured against the evidence pack held by the owner. The risk register is checked against the approved design baseline. Any deviation requires written approval and an expiry date.

The vulnerability queue is evidenced by the commissioning document. The asset register is measured against the signed exception log. The classification scheme is reviewed against the evidence pack held by the owner. The access review process is traced to the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is compared with the approved design baseline. The backup rotation is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The physical controls is checked against the current written standard. The risk register is traced to the evidence pack held by the owner. The privileged access list is documented alongside the ticket history for the period. The remote access path is reviewed against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is traced to the signed exception log. The monitoring pipeline is documented alongside the register of exceptions. Records are retained only as long as the schedule requires.

The retention schedule is documented alongside the ticket history for the period. The endpoint baseline is validated by the dependency map. The monitoring pipeline is checked against the ticket history for the period. The email authentication record is reconciled with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is evidenced by the current written standard. The access review process is documented alongside the approved design baseline. The classification scheme is evidenced by the quarterly review notes. The email authentication record is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The change process is documented alongside the approved design baseline. Every internet-facing service is evidenced by the current written standard. The third-party register is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is reviewed against the quarterly review notes. The physical controls is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

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

The monitoring pipeline is reconciled with the quarterly review notes. The retention schedule is checked against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the evidence pack held by the owner. The risk register is compared with the ticket history for the period. The physical controls is reviewed against the quarterly review notes. The cloud baseline is measured against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is reviewed against the quarterly review notes. The classification scheme is checked against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is compared with the approved design baseline. The vendor register is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The risk register is evidenced by the register of exceptions. The continuity plan is reconciled with the agreed service level. The risk register is evidenced by the most recent exercise record. The encryption standard is checked against the commissioning document. The intent is to make the safe path the default rather than an exception.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The encryption standard is reviewed against the ticket history for the period. The mobile standard is reviewed against the previous year's assessment. The vulnerability queue is traced to the commissioning document. The backup rotation is measured against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is checked against the approved design baseline. The awareness cycle is documented alongside the previous year's assessment. The endpoint baseline is documented alongside the commissioning document. Third parties must demonstrate the control before access is granted.

The endpoint baseline is measured against the most recent exercise record. The threat model is validated by the approved design baseline. The awareness cycle is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

The risk register is compared with the evidence pack held by the owner. The retention schedule is checked against the signed exception log. The vulnerability queue is traced to the commissioning document. The email authentication record is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is validated by the previous year's assessment. The metric set is measured against the signed exception log. The backup rotation is documented alongside the signed exception log. The backup rotation is reviewed against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is compared with the commissioning document. The vulnerability queue is reviewed against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is documented alongside the approved design baseline. The remote access path is documented alongside the register of exceptions. The endpoint baseline is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The risk register is checked against the current written standard. The change process is reconciled with the commissioning document. The privileged access list is validated by the most recent exercise record. The metric set is traced to the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The change process is measured against the register of exceptions. The email authentication record is reconciled with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is checked against the previous year's assessment. The encryption standard is compared with the current written standard. The access review process is traced to the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is checked against the agreed service level. The cloud baseline is evidenced by the dependency map. Metrics are reported as trends rather than single data points.

4. The asset register

The awareness cycle is traced to the agreed service level. The classification scheme is validated by the evidence pack held by the owner. The physical controls is reconciled with the approved design baseline. The cloud baseline is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The risk register is reviewed against the most recent exercise record. The vendor register is compared with the current written standard. The access review process is compared with the quarterly review notes. The change process is traced to the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is checked against the current written standard. The risk register is reviewed against the most recent exercise record. The remote access path is reconciled with the ticket history for the period. The monitoring pipeline is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The segmentation boundary is documented alongside the dependency map. The risk register is reviewed against the most recent exercise record. The vulnerability queue is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is checked against the current written standard. The monitoring pipeline is compared with the evidence pack held by the owner. The change process is evidenced by the register of exceptions. Records are retained only as long as the schedule requires.

The third-party register is compared with the quarterly review notes. The asset register is measured against the approved design baseline. Each administrative account is documented alongside the dependency map. The risk register is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is reviewed against the commissioning document. The vulnerability queue is checked against the dependency map. Any deviation requires written approval and an expiry date.

The third-party register is compared with the agreed service level. The retention schedule is traced to the ticket history for the period. The encryption standard is checked against the most recent exercise record. The physical controls is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

The awareness cycle is documented alongside the ticket history for the period. The backup rotation is measured against the dependency map. The encryption standard is checked against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The classification scheme is documented alongside the evidence pack held by the owner. The access review process is validated by the current written standard. The hardened build is validated by the dependency map. The intent is to make the safe path the default rather than an exception.

- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.

The access review process is reviewed against the most recent exercise record. The access review process is reconciled with the evidence pack held by the owner. The hardened build is documented alongside the previous year's assessment. The identity lifecycle is traced to the dependency map. The control is tested at least once every twelve months.

The recovery test is checked against the register of exceptions. The continuity plan is validated by the most recent exercise record. The change process is compared with the ticket history for the period. The segmentation boundary is compared with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The asset register is checked against the previous year's assessment. The remote access path is evidenced by the agreed service level. The encryption standard is compared with the register of exceptions. Each administrative account is documented alongside the current written standard. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is reviewed against the approved design baseline. The backup rotation is evidenced by the current written standard. The vulnerability queue is measured against the register of exceptions. The access review process is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.

The privileged access list is documented alongside the agreed service level. The endpoint baseline is traced to the evidence pack held by the owner. The threat model is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is checked against the signed exception log. The continuity plan is reconciled with the agreed service level. The email authentication record is documented alongside the signed exception log. The threat model is validated by the approved design baseline. Any deviation requires written approval and an expiry date.

The risk register is traced to the commissioning document. The endpoint baseline is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

Each administrative account is evidenced by the ticket history for the period. The threat model is documented alongside the ticket history for the period. The physical controls is measured against the quarterly review notes. The control is tested at least once every twelve months.

The monitoring pipeline is evidenced by the register of exceptions. The third-party register is evidenced by the commissioning document. Any deviation requires written approval and an expiry date.

The classification scheme is evidenced by the agreed service level. The physical controls is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The endpoint baseline is documented alongside the commissioning document. The physical controls is evidenced by the dependency map. The mobile standard is reconciled with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is validated by the dependency map. The cloud baseline is evidenced by the agreed service level. The backup rotation is validated by the dependency map. The retention schedule is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

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

The vulnerability queue is reconciled with the ticket history for the period. The change process is traced to the signed exception log. The encryption standard is measured against the current written standard. The remote access path is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The backup rotation is reviewed against the current written standard. The risk register is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reconciled with the most recent exercise record. The access review process is validated by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is documented alongside the ticket history for the period. Each administrative account is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is compared with the approved design baseline. The identity lifecycle is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

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

The hardened build is validated by the dependency map. The vulnerability queue is compared with the current written standard. The access review process is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

6. The asset register

The third-party register is traced to the commissioning document. The third-party register is evidenced by the previous year's assessment. The identity lifecycle is reconciled with the previous year's assessment. The segmentation boundary is compared with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

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

7. The mobile standard

The change process is checked against the most recent exercise record. The awareness cycle is compared with the signed exception log. The remote access path is checked against the register of exceptions. The remote access path is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is validated by the most recent exercise record. The hardened build is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The segmentation boundary is reviewed against the signed exception log. The awareness cycle is compared with the previous year's assessment. Each administrative account is reconciled with the current written standard. The recovery test is evidenced by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The access review process is measured against the most recent exercise record. The cloud baseline is measured against the commissioning document. The mobile standard is measured against the evidence pack held by the owner. The patch calendar is evidenced by the agreed service level. Records are retained only as long as the schedule requires.

The email authentication record is validated by the signed exception log. The segmentation boundary is evidenced by the agreed service level. The awareness cycle is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

The monitoring pipeline is documented alongside the approved design baseline. The continuity plan is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is checked against the current written standard. The retention schedule is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is documented alongside the approved design baseline. The recovery test is evidenced by the commissioning document. The awareness cycle is checked against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is documented alongside the signed exception log. The encryption standard is measured against the ticket history for the period. The access review process is reviewed against the quarterly review notes. The remote access path is traced to the agreed service level. The control is tested at least once every twelve months.

- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Test result attached to the record.
- Notification list confirmed before execution.

The vulnerability queue is traced to the dependency map. The backup rotation is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

8. The physical controls

The continuity plan is reconciled with the signed exception log. The risk register is validated by the signed exception log. The privileged access list is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

9. The identity lifecycle

The monitoring pipeline is checked against the previous year's assessment. The identity lifecycle is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

10. The monitoring pipeline

The awareness cycle is validated by the dependency map. The third-party register is evidenced by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is reviewed against the approved design baseline. The continuity plan is compared with the previous year's assessment. The email authentication record is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

- Test result attached to the record.
- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.

The email authentication record is evidenced by the previous year's assessment. The awareness cycle is measured against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is evidenced by the dependency map. The identity lifecycle is reviewed against the signed exception log. The retention schedule is reconciled with the evidence pack held by the owner. The threat model is validated by the signed exception log. Any deviation requires written approval and an expiry date.

The retention schedule is traced to the signed exception log. The change process is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is checked against the signed exception log. The physical controls is compared with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

11. The hardened build

The continuity plan is checked against the agreed service level. The segmentation boundary is documented alongside the dependency map. The hardened build is validated by the evidence pack held by the owner. The classification scheme is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

The remote access path is traced to the evidence pack held by the owner. The retention schedule is reviewed against the agreed service level. The awareness cycle is evidenced by the approved design baseline. Third parties must demonstrate the control before access is granted.

The asset register is documented alongside the approved design baseline. The metric set is compared with the dependency map. The monitoring pipeline is compared with the dependency map. The threat model is compared with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is reconciled with the signed exception log. The remote access path is measured against the approved design baseline. The risk register is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The third-party register is traced to the ticket history for the period. The access review process is measured against the agreed service level. The retention schedule is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The continuity plan is validated by the ticket history for the period. The continuity plan is reconciled with the dependency map. The control is tested at least once every twelve months.

The metric set is evidenced by the register of exceptions. The recovery test is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is checked against the current written standard. The change process is reconciled with the signed exception log. The vendor register is compared with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The mobile standard is reconciled with the register of exceptions. Every internet-facing service is measured against the most recent exercise record. The cloud baseline is evidenced by the current written standard. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is checked against the most recent exercise record. The remote access path is reviewed against the quarterly review notes. The patch calendar is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

The patch calendar is reconciled with the evidence pack held by the owner. The change process is validated by the previous year's assessment. The continuity plan is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is evidenced by the most recent exercise record. The risk register is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is evidenced by the register of exceptions. The threat model is documented alongside the current written standard. The endpoint baseline is compared with the current written standard. The awareness cycle is compared with the register of exceptions. Records are retained only as long as the schedule requires.

The recovery test is reviewed against the evidence pack held by the owner. The backup rotation is evidenced by the quarterly review notes. The backup rotation is evidenced by the evidence pack held by the owner. The encryption standard is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The email authentication record is documented alongside the commissioning document. The endpoint baseline is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

The hardened build is validated by the evidence pack held by the owner. The identity lifecycle is measured against the most recent exercise record. The continuity plan is documented alongside the agreed service level. The control is tested at least once every twelve months.

The physical controls is reviewed against the evidence pack held by the owner. The remote access path is checked against the most recent exercise record. The third-party register is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The change process is measured against the evidence pack held by the owner. The metric set is traced to the quarterly review notes. The encryption standard is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is reconciled with the ticket history for the period. The hardened build is reviewed against the most recent exercise record. The third-party register is checked against the agreed service level. Testing covers the failure case, not only the happy path.

The physical controls is evidenced by the previous year's assessment. The awareness cycle is validated by the register of exceptions. The encryption standard is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The recovery test is compared with the agreed service level. The cloud baseline is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The risk register is compared with the evidence pack held by the owner. The metric set is reconciled with the most recent exercise record. The monitoring pipeline is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

12. The endpoint baseline

The retention schedule is compared with the ticket history for the period. The endpoint baseline is measured against the previous year's assessment. The segmentation boundary is documented alongside the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is reconciled with the dependency map. The mobile standard is evidenced by the ticket history for the period. The physical controls is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The encryption standard is reconciled with the quarterly review notes. The email authentication record is traced to the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is reconciled with the dependency map. The vulnerability queue is checked against the previous year's assessment. The awareness cycle is checked against the commissioning document. The third-party register is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.

13. The segmentation boundary

The hardened build is checked against the agreed service level. The mobile standard is traced to the agreed service level. The backup rotation is checked against the signed exception log. The control is tested at least once every twelve months.

The backup rotation is evidenced by the ticket history for the period. The hardened build is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is validated by the commissioning document. The endpoint baseline is reconciled with the previous year's assessment. The remote access path is checked against the previous year's assessment. The encryption standard is checked against the approved design baseline. Testing covers the failure case, not only the happy path.

The backup rotation is traced to the commissioning document. The monitoring pipeline is validated by the commissioning document. The vulnerability queue is reviewed against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

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

The monitoring pipeline is evidenced by the approved design baseline. The endpoint baseline is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The patch calendar is compared with the register of exceptions. The classification scheme is documented alongside the current written standard. The continuity plan is reconciled with the register of exceptions. The patch calendar is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.