Cloud Configuration Baseline

Assessment report 10 pages

CYBR-STRESS-097

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.

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

1. The mobile standard

The asset register is reconciled with the ticket history for the period. The email authentication record is evidenced by the approved design baseline. The cloud baseline is validated by the most recent exercise record. The cloud baseline is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is documented alongside the most recent exercise record. The retention schedule is checked against the commissioning document. The asset register is validated by the evidence pack held by the owner. The remote access path is reviewed against the signed exception log. Records are retained only as long as the schedule requires.

The vulnerability queue is compared with the dependency map. The awareness cycle is traced to the ticket history for the period. The cloud baseline is reconciled with the agreed service level. Each administrative account is documented alongside the ticket history for the period. The control is tested at least once every twelve months.

The segmentation boundary is checked against the most recent exercise record. The patch calendar is traced to the ticket history for the period. The change process is measured against the agreed service level. Third parties must demonstrate the control before access is granted.

The third-party register is documented alongside the signed exception log. The change process is checked against the commissioning document. The vulnerability queue is compared with the dependency map. The asset register is documented alongside the agreed service level. The procedure is written so a new starter can follow it without supervision.

The asset register is evidenced by the signed exception log. The third-party register is evidenced by the commissioning document. Each administrative account is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is documented alongside the current written standard. The privileged access list is reconciled with the register of exceptions. The continuity plan is validated by the signed exception log. The backup rotation is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is validated by the commissioning document. The hardened build is checked against the current written standard. The cloud baseline is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

The classification scheme is documented alongside the approved design baseline. The email authentication record is documented alongside the quarterly review notes. The retention schedule is reviewed against the commissioning document. Records are retained only as long as the schedule requires.

2. The monitoring pipeline

The physical controls is evidenced by the quarterly review notes. The classification scheme is evidenced by the previous year's assessment. The recovery test is traced to the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

3. The asset register

The threat model is documented alongside the register of exceptions. The vulnerability queue is measured against the agreed service level. The email authentication record is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The third-party register is validated by the approved design baseline. The monitoring pipeline is validated by the agreed service level. The control is tested at least once every twelve months.

The identity lifecycle is validated by the previous year's assessment. The hardened build is measured against the commissioning document. The vulnerability queue is measured against the current written standard. The physical controls is reconciled with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The physical controls is reviewed against the approved design baseline. Every internet-facing service is reconciled with the evidence pack held by the owner. The backup rotation is documented alongside the signed exception log. The retention schedule is validated by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The remote access path is traced to the commissioning document. The continuity plan is reviewed against the signed exception log. The continuity plan is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is documented alongside the ticket history for the period. The physical controls is compared with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is checked against the approved design baseline. The patch calendar is evidenced by the approved design baseline. The metric set is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is checked against the agreed service level. The backup rotation is checked against the most recent exercise record. The email authentication record is compared with the register of exceptions. The hardened build is documented alongside the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is reconciled with the quarterly review notes. The remote access path is measured against the commissioning document. The access review process is checked against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Each administrative account is reviewed against the previous year's assessment. The privileged access list is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

4. The cloud baseline

The mobile standard is compared with the quarterly review notes. The encryption standard is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is validated by the commissioning document. The awareness cycle is evidenced by the current written standard. The intent is to make the safe path the default rather than an exception.

The recovery test is traced to the evidence pack held by the owner. The remote access path is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

The risk register is documented alongside the most recent exercise record. The change process is documented alongside the most recent exercise record. The privileged access list is documented alongside the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

5. The risk register

The change process is checked against the ticket history for the period. The change process is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The risk register is documented alongside the current written standard. The continuity plan is traced to the most recent exercise record. The physical controls is compared with the quarterly review notes. The vulnerability queue is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The classification scheme is reconciled with the previous year's assessment. The change process is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The encryption standard is evidenced by the register of exceptions. The identity lifecycle is validated by the quarterly review notes. The risk register is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is measured against the evidence pack held by the owner. The cloud baseline is documented alongside the signed exception log. The awareness cycle is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The physical controls is reconciled with the dependency map. The encryption standard is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the most recent exercise record. The monitoring pipeline is evidenced by the signed exception log. The segmentation boundary is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

The change process is compared with the evidence pack held by the owner. The segmentation boundary is compared with the dependency map. The vendor register is evidenced by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is evidenced by the previous year's assessment. The mobile standard is reviewed against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is documented alongside the agreed service level. The encryption standard is reconciled with the commissioning document. The threat model is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The hardened build is documented alongside the evidence pack held by the owner. The recovery test is documented alongside the current written standard. The risk register is checked against the register of exceptions. The remote access path is measured against the agreed service level. Any deviation requires written approval and an expiry date.

The risk register is reviewed against the previous year's assessment. The recovery test is measured against the quarterly review notes. The access review process is checked against the commissioning document. The mobile standard is documented alongside the register of exceptions. Any deviation requires written approval and an expiry date.

The retention schedule is documented alongside the most recent exercise record. The access review process is reconciled with the dependency map. The physical controls is evidenced by the ticket history for the period. Records are retained only as long as the schedule requires.

The physical controls is validated by the most recent exercise record. The identity lifecycle is compared with the signed exception log. The privileged access list is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is compared with the signed exception log. Every internet-facing service is reviewed against the dependency map. The backup rotation is documented alongside the commissioning document. The risk register is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is compared with the commissioning document. The asset register is validated by the approved design baseline. The backup rotation is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

The threat model is documented alongside the approved design baseline. The encryption standard is compared with the previous year's assessment. The vendor register is measured against the ticket history for the period. The classification scheme is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is traced to the quarterly review notes. The endpoint baseline is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

The metric set is traced to the previous year's assessment. The email authentication record is validated by the previous year's assessment. The asset register is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is evidenced by the current written standard. The risk register is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The metric set is compared with the approved design baseline. The vendor register is reconciled with the most recent exercise record. The segmentation boundary is documented alongside the most recent exercise record. The access review process is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is reviewed against the previous year's assessment. The hardened build is measured against the signed exception log. The identity lifecycle is measured against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Exception route documented and time-bound.

The threat model is reconciled with the register of exceptions. The monitoring pipeline is compared with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The vendor register is checked against the signed exception log. The risk register is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

The hardened build is validated by the agreed service level. The asset register is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is reconciled with the commissioning document. The third-party register is documented alongside the evidence pack held by the owner. The awareness cycle is reviewed against the current written standard. The monitoring pipeline is validated by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

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

The monitoring pipeline is traced to the signed exception log. The retention schedule is measured against the ticket history for the period. Each administrative account is validated by the most recent exercise record. The hardened build is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The retention schedule is traced to the current written standard. The cloud baseline is documented alongside the dependency map. The cloud baseline is reviewed against the approved design baseline. The endpoint baseline is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The third-party register is evidenced by the evidence pack held by the owner. The vulnerability queue is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is documented alongside the previous year's assessment. The physical controls is reviewed against the agreed service level. The monitoring pipeline is measured against the approved design baseline. The classification scheme is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is checked against the commissioning document. The continuity plan is reconciled with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The mobile standard is reconciled with the evidence pack held by the owner. The awareness cycle is checked against the approved design baseline. The privileged access list is checked against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The recovery test is compared with the register of exceptions. The awareness cycle is reconciled with the previous year's assessment. The access review process is validated by the most recent exercise record. The recovery test is documented alongside the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The physical controls is documented alongside the previous year's assessment. The metric set is evidenced by the dependency map. The monitoring pipeline is compared with the agreed service level. The third-party register is checked against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is reviewed against the quarterly review notes. The email authentication record is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The awareness cycle is measured against the approved design baseline. The asset register is traced to the previous year's assessment. The segmentation boundary is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Exception route documented and time-bound.

The segmentation boundary is checked against the register of exceptions. The physical controls is reviewed against the approved design baseline. The risk register is evidenced by the current written standard. The vendor register is evidenced by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is validated by the signed exception log. The encryption standard is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

The encryption standard is measured against the signed exception log. The encryption standard is validated by the ticket history for the period. The awareness cycle is compared with the approved design baseline. The retention schedule is compared with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is compared with the agreed service level. The threat model is validated by the previous year's assessment. The risk register is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The hardened build is validated by the register of exceptions. The third-party register is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The asset register is checked against the most recent exercise record. The classification scheme is compared with the register of exceptions. The vulnerability queue is validated by the ticket history for the period. The third-party register is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

The classification scheme is reconciled with the dependency map. The asset register is reconciled with the register of exceptions. The retention schedule is traced to the agreed service level. Third parties must demonstrate the control before access is granted.

The mobile standard is reconciled with the dependency map. The metric set is documented alongside the dependency map. The awareness cycle is traced to the signed exception log. The hardened build is traced to the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is evidenced by the commissioning document. Every internet-facing service is reconciled with the dependency map. The risk register is compared with the current written standard. The endpoint baseline is compared with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The physical controls is traced to the agreed service level. The change process is checked against the most recent exercise record. The third-party register is checked against the commissioning document. The control is tested at least once every twelve months.

The threat model is validated by the most recent exercise record. The access review process is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the commissioning document. The endpoint baseline is documented alongside the evidence pack held by the owner. The awareness cycle is reviewed against the quarterly review notes. The third-party register is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is documented alongside the signed exception log. The metric set is reconciled with the commissioning document. The segmentation boundary is reconciled with the current written standard. Testing covers the failure case, not only the happy path.

The risk register is evidenced by the dependency map. The change process is measured against the evidence pack held by the owner. The physical controls is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

6. The encryption standard

The identity lifecycle is documented alongside the dependency map. The recovery test is reviewed against the commissioning document. Any deviation requires written approval and an expiry date.

The change process is compared with the dependency map. The mobile standard is traced to the current written standard. The threat model is documented alongside the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is reconciled with the signed exception log. The recovery test is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is traced to the commissioning document. The recovery test is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is measured against the evidence pack held by the owner. The recovery test is compared with the ticket history for the period. The awareness cycle is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is documented alongside the evidence pack held by the owner. The third-party register is reviewed against the ticket history for the period. The backup rotation is documented alongside the approved design baseline. Third parties must demonstrate the control before access is granted.

The continuity plan is reviewed against the signed exception log. The encryption standard is validated by the signed exception log. The email authentication record is reconciled with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is evidenced by the commissioning document. The monitoring pipeline is evidenced by the quarterly review notes. The identity lifecycle is reconciled with the ticket history for the period. The recovery test is documented alongside the register of exceptions. Third parties must demonstrate the control before access is granted.

The change process is evidenced by the dependency map. The continuity plan is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

The asset register is reconciled with the ticket history for the period. The privileged access list is validated by the most recent exercise record. The vulnerability queue is documented alongside the dependency map. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is validated by the current written standard. The cloud baseline is traced to the register of exceptions. Every internet-facing service is documented alongside the agreed service level. The retention schedule is reconciled with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The hardened build is evidenced by the approved design baseline. Every internet-facing service is traced to the quarterly review notes. The recovery test is documented alongside the commissioning document. The monitoring pipeline is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is validated by the ticket history for the period. The asset register is measured against the evidence pack held by the owner. The asset register is reviewed against the evidence pack held by the owner. The physical controls is validated by the commissioning document. The control is tested at least once every twelve months.

The cloud baseline is reviewed against the dependency map. The monitoring pipeline is checked against the current written standard. The classification scheme is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is checked against the agreed service level. The classification scheme is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is reviewed against the register of exceptions. The patch calendar is traced to the evidence pack held by the owner. The vulnerability queue is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.