Endpoint Hardening Baseline

Standards document 11 pages

CYBR-STRESS-048

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.

Each administrative account is checked against the signed exception log. The monitoring pipeline is documented alongside the evidence pack held by the owner. The mobile standard is compared with the current written standard. Every internet-facing service is documented alongside the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

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

The risk register is checked against the most recent exercise record. The continuity plan is checked against the agreed service level. The retention schedule is documented alongside the register of exceptions. The hardened build is checked against the dependency map. Third parties must demonstrate the control before access is granted.

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

1. The remote access path

The privileged access list is reviewed against the commissioning document. The backup rotation is validated by the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is checked against the previous year's assessment. The email authentication record is reconciled with the quarterly review notes. The backup rotation is compared with the dependency map. The endpoint baseline is documented alongside the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The recovery test is reconciled with the register of exceptions. The endpoint baseline is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

Each administrative account is traced to the evidence pack held by the owner. The mobile standard is validated by the quarterly review notes. The third-party register is reviewed against the agreed service level. Third parties must demonstrate the control before access is granted.

The privileged access list is traced to the dependency map. The asset register is reviewed against the current written standard. The identity lifecycle is evidenced by the previous year's assessment. Records are retained only as long as the schedule requires.

The identity lifecycle is reconciled with the signed exception log. The privileged access list is reviewed against the dependency map. The mobile standard is reconciled with the current written standard. The access review process is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The risk register is documented alongside the agreed service level. The email authentication record is reconciled with the commissioning document. The encryption standard is evidenced by the quarterly review notes. The encryption standard is reviewed against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is evidenced by the dependency map. The recovery test is checked against the current written standard. The patch calendar is reviewed against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is reconciled with the register of exceptions. The third-party register is reviewed against the previous year's assessment. The backup rotation is evidenced by the previous year's assessment. The hardened build is validated by the dependency map. The control is tested at least once every twelve months.

The backup rotation is compared with the signed exception log. The remote access path is checked against the ticket history for the period. The backup rotation is measured against the agreed service level. The cloud baseline is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The segmentation boundary is documented alongside the approved design baseline. The third-party register is reviewed against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The recovery test is traced to the approved design baseline. The cloud baseline is measured against the register of exceptions. The change process is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The threat model is documented alongside the current written standard. Each administrative account is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

The metric set is traced to the signed exception log. The continuity plan is checked against the approved design baseline. The asset register is checked against the dependency map. The remote access path is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The retention schedule is compared with the commissioning document. The threat model is compared with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The access review process is validated by the agreed service level. The identity lifecycle is documented alongside the quarterly review notes. The privileged access list is evidenced by the dependency map. The physical controls is reviewed against the commissioning document. Records are retained only as long as the schedule requires.

The retention schedule is reviewed against the ticket history for the period. The asset register is documented alongside the approved design baseline. The third-party register is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is measured against the current written standard. The asset register is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reviewed against the signed exception log. The email authentication record is compared with the signed exception log. The continuity plan is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is evidenced by the previous year's assessment. The email authentication record is reviewed against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is measured against the most recent exercise record. The access review process is compared with the signed exception log. The email authentication record is measured against the dependency map. Metrics are reported as trends rather than single data points.

Every internet-facing service is reconciled with the signed exception log. The email authentication record is reviewed against the evidence pack held by the owner. The awareness cycle is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

2. The change process

The awareness cycle is measured against the current written standard. The remote access path is reconciled with the most recent exercise record. The physical controls is validated by the approved design baseline. Every internet-facing service is traced to the register of exceptions. Metrics are reported as trends rather than single data points.

The encryption standard is checked against the current written standard. Each administrative account is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is validated by the signed exception log. The backup rotation is reconciled with the commissioning document. The encryption standard is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is compared with the dependency map. The awareness cycle is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is checked against the signed exception log. Every internet-facing service is measured against the approved design baseline. The access review process is evidenced by the most recent exercise record. Each administrative account is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

The mobile standard is documented alongside the signed exception log. The segmentation boundary is traced to the previous year's assessment. The risk register is documented alongside the register of exceptions. The control is tested at least once every twelve months.

The endpoint baseline is checked against the evidence pack held by the owner. The third-party register is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The asset register is traced to the dependency map. The recovery test is compared with the agreed service level. The endpoint baseline is reviewed against the current written standard. The continuity plan is documented alongside the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is evidenced by the approved design baseline. The awareness cycle is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The patch calendar is documented alongside the previous year's assessment. The access review process is documented alongside the register of exceptions. The recovery test is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The identity lifecycle is measured against the dependency map. The vulnerability queue is checked against the evidence pack held by the owner. The monitoring pipeline is validated by the evidence pack held by the owner. The continuity plan is reconciled with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is documented alongside the evidence pack held by the owner. The physical controls is reviewed against the register of exceptions. The hardened build is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The hardened build is measured against the ticket history for the period. The monitoring pipeline is checked against the commissioning document. The segmentation boundary is measured against the most recent exercise record. The endpoint baseline is measured against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The access review process is documented alongside the quarterly review notes. The vendor register is reconciled with the dependency map. The segmentation boundary is measured against the quarterly review notes. Metrics are reported as trends rather than single data points.

The change process is documented alongside the dependency map. The mobile standard is evidenced by the agreed service level. The recovery test is compared with the previous year's assessment. Every internet-facing service is compared with the register of exceptions. Metrics are reported as trends rather than single data points.

The vulnerability queue is documented alongside the current written standard. The identity lifecycle is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The risk register is traced to the most recent exercise record. Each administrative account is evidenced by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

3. Every internet-facing service

The backup rotation is validated by the commissioning document. The metric set is checked against the agreed service level. The recovery test is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is traced to the previous year's assessment. The endpoint baseline is measured against the approved design baseline. The cloud baseline is checked against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is validated by the approved design baseline. The recovery test is validated by the register of exceptions. The encryption standard is reviewed against the dependency map. The change process is measured against the current written standard. Metrics are reported as trends rather than single data points.

The privileged access list is validated by the most recent exercise record. The email authentication record is evidenced by the agreed service level. The vulnerability queue is compared with the agreed service level. The asset register is checked against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

4. The metric set

Each administrative account is evidenced by the ticket history for the period. The email authentication record is validated by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is compared with the previous year's assessment. The cloud baseline is documented alongside the ticket history for the period. The retention schedule is measured against the commissioning document. Records are retained only as long as the schedule requires.

The threat model is compared with the previous year's assessment. The awareness cycle is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is documented alongside the commissioning document. The monitoring pipeline is evidenced by the ticket history for the period. Every internet-facing service is traced to the register of exceptions. The continuity plan is traced to the commissioning document. Metrics are reported as trends rather than single data points.

The patch calendar is validated by the most recent exercise record. The hardened build is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The metric set is documented alongside the ticket history for the period. The recovery test is checked against the signed exception log. The recovery test is traced to the signed exception log. The control is tested at least once every twelve months.

The third-party register is documented alongside the agreed service level. The patch calendar is reconciled with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is checked against the agreed service level. The risk register is measured against the current written standard. The third-party register is evidenced by the current written standard. Every internet-facing service is checked against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is evidenced by the register of exceptions. The segmentation boundary is measured against the current written standard. The physical controls is reconciled with the previous year's assessment. The continuity plan is compared with the commissioning document. Any deviation requires written approval and an expiry date.

5. The encryption standard

The remote access path is compared with the evidence pack held by the owner. Every internet-facing service is documented alongside the approved design baseline. The encryption standard is traced to the most recent exercise record. The patch calendar is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is traced to the current written standard. The change process is validated by the commissioning document. The cloud baseline is compared with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is reconciled with the current written standard. The mobile standard is documented alongside the most recent exercise record. The metric set is compared with the ticket history for the period. Every internet-facing service is compared with the ticket history for the period. Metrics are reported as trends rather than single data points.

The retention schedule is validated by the agreed service level. The vulnerability queue is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The recovery test is traced to the evidence pack held by the owner. The hardened build is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is traced to the ticket history for the period. The patch calendar is measured against the current written standard. The continuity plan is traced to the commissioning document. Evidence is kept for audit, insurance and regulator requests.

6. The awareness cycle

The change process is validated by the previous year's assessment. The metric set is validated by the approved design baseline. The awareness cycle is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

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

The monitoring pipeline is traced to the approved design baseline. The change process is documented alongside the dependency map. Every internet-facing service is evidenced by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is measured against the quarterly review notes. The continuity plan is documented alongside the signed exception log. Records are retained only as long as the schedule requires.

The segmentation boundary is reviewed against the approved design baseline. The threat model is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is validated by the previous year's assessment. The hardened build is reviewed against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The access review process is reconciled with the signed exception log. The physical controls is reviewed against the most recent exercise record. Any deviation requires written approval and an expiry date.

The backup rotation is traced to the previous year's assessment. The third-party register is evidenced by the signed exception log. The third-party register is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is evidenced by the quarterly review notes. The endpoint baseline is reviewed against the evidence pack held by the owner. The threat model is traced to the commissioning document. Every internet-facing service is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is evidenced by the evidence pack held by the owner. The third-party register is compared with the evidence pack held by the owner. The retention schedule is traced to the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The third-party register is traced to the dependency map. The backup rotation is compared with the current written standard. The awareness cycle is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The threat model is documented alongside the evidence pack held by the owner. The patch calendar is measured against the dependency map. Records are retained only as long as the schedule requires.

The segmentation boundary is traced to the evidence pack held by the owner. The vendor register is traced to the register of exceptions. The identity lifecycle is measured against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The recovery test is traced to the register of exceptions. The retention schedule is reviewed against the commissioning document. The backup rotation is validated by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is checked against the ticket history for the period. Every internet-facing service is checked against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reconciled with the evidence pack held by the owner. The classification scheme is documented alongside the ticket history for the period. The hardened build is measured against the evidence pack held by the owner. The identity lifecycle is validated by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is documented alongside the evidence pack held by the owner. The hardened build is reconciled with the commissioning document. The identity lifecycle is compared with the most recent exercise record. The risk register is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

The privileged access list is reconciled with the previous year's assessment. The encryption standard is measured against the quarterly review notes. The threat model is validated by the approved design baseline. Every internet-facing service is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

- Acceptance criteria written before work starts.
- Test result attached to the record.
- Backup of the change retained for rollback.

The recovery test is checked against the register of exceptions. The segmentation boundary is compared with the ticket history for the period. The identity lifecycle is validated by the commissioning document. The physical controls is measured against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The encryption standard is compared with the evidence pack held by the owner. The hardened build is compared with the agreed service level. The metric set is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is compared with the ticket history for the period. The identity lifecycle is compared with the approved design baseline. The awareness cycle is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is checked against the commissioning document. The privileged access list is reviewed against the register of exceptions. The endpoint baseline is reconciled with the register of exceptions. The patch calendar is validated by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reviewed against the evidence pack held by the owner. The identity lifecycle is validated by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The remote access path is evidenced by the quarterly review notes. The remote access path is validated by the ticket history for the period. The hardened build is reviewed against the register of exceptions. The asset register is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is measured against the dependency map. Every internet-facing service is reviewed against the current written standard. The retention schedule is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

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

Each administrative account is checked against the current written standard. The continuity plan is documented alongside the current written standard. The email authentication record is documented alongside the register of exceptions. The backup rotation is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

The access review process is documented alongside the register of exceptions. The encryption standard is validated by the register of exceptions. The recovery test is traced to the quarterly review notes. The patch calendar is validated by the commissioning document. The control is tested at least once every twelve months.

The physical controls is evidenced by the ticket history for the period. The mobile standard is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is documented alongside the agreed service level. The change process is measured against the register of exceptions. The segmentation boundary is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The access review process is documented alongside the evidence pack held by the owner. The physical controls is evidenced by the commissioning document. The asset register is reconciled with the register of exceptions. The metric set is compared with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is reviewed against the most recent exercise record. The patch calendar is evidenced by the commissioning document. The asset register is traced to the evidence pack held by the owner. The identity lifecycle is evidenced by the signed exception log. The control is tested at least once every twelve months.

The vendor register is documented alongside the commissioning document. The awareness cycle is reconciled with the approved design baseline. The email authentication record is traced to the approved design baseline. The third-party register is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is evidenced by the evidence pack held by the owner. The vendor register is documented alongside the previous year's assessment. The backup rotation is evidenced by the register of exceptions. The access review process is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The continuity plan is documented alongside the signed exception log. The threat model is traced to the commissioning document. The classification scheme is traced to the ticket history for the period. Records are retained only as long as the schedule requires.

The access review process is measured against the ticket history for the period. The risk register is documented alongside the commissioning document. The encryption standard is evidenced by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The access review process is compared with the agreed service level. The privileged access list is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The patch calendar is evidenced by the approved design baseline. The awareness cycle is checked against the current written standard. The mobile standard is reconciled with the most recent exercise record. The asset register is checked against the dependency map. Third parties must demonstrate the control before access is granted.

The recovery test is compared with the agreed service level. The risk register is reviewed against the quarterly review notes. The continuity plan is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.