Endpoint Hardening Programme

Benchmark document 14 pages

CYBR-STRESS-065

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 identity lifecycle is evidenced by the previous year's assessment. The metric set is evidenced by the ticket history for the period. The asset register is evidenced by the most recent exercise record. The remote access path is validated by the agreed service level. Any deviation requires written approval and an expiry date.

The risk register is documented alongside the evidence pack held by the owner. Every internet-facing service is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is evidenced by the evidence pack held by the owner. The change process is checked against the ticket history for the period. The continuity plan is evidenced by the dependency map. The control is tested at least once every twelve months.

Every internet-facing service is checked against the evidence pack held by the owner. The identity lifecycle is evidenced by the previous year's assessment. The vulnerability queue is reviewed against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The recovery test is compared with the quarterly review notes. The vulnerability queue is reconciled with the register of exceptions. The email authentication record is measured against the dependency map. The classification scheme is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is validated by the approved design baseline. The vulnerability queue is evidenced by the dependency map. The hardened build is documented alongside the register of exceptions. The continuity plan is reconciled with the previous year's assessment. The control is tested at least once every twelve months.

- Escalation path agreed with the service owner.
- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Review date scheduled and visible.

The classification scheme is traced to the current written standard. The backup rotation is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

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

The vendor register is reconciled with the quarterly review notes. The segmentation boundary is reviewed against the signed exception log. The segmentation boundary is traced to the dependency map. The metric set is checked against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is documented alongside the most recent exercise record. The cloud baseline is traced to the evidence pack held by the owner. The threat model is reconciled with the current written standard. The patch calendar is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

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

The identity lifecycle is reconciled with the approved design baseline. Each administrative account is traced to the agreed service level. The privileged access list is evidenced by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The access review process is documented alongside the quarterly review notes. The third-party register is traced to the approved design baseline. Third parties must demonstrate the control before access is granted.

The identity lifecycle is validated by the signed exception log. The retention schedule is measured against the evidence pack held by the owner. The retention schedule is reconciled with the previous year's assessment. The risk register is checked against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The threat model is validated by the quarterly review notes. The access review process is measured against the current written standard. The third-party register is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is traced to the commissioning document. The patch calendar is measured against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is documented alongside the current written standard. The patch calendar is compared with the dependency map. Testing covers the failure case, not only the happy path.

The remote access path is checked against the agreed service level. The monitoring pipeline is reviewed against the ticket history for the period. The privileged access list is documented alongside the approved design baseline. The recovery test is reconciled with the current written standard. Records are retained only as long as the schedule requires.

Each administrative account is reviewed against the commissioning document. The retention schedule is checked against the dependency map. The third-party register is measured against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is checked against the dependency map. The hardened build is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is reconciled with the evidence pack held by the owner. The third-party register is validated by the evidence pack held by the owner. The mobile standard is documented alongside the quarterly review notes. The patch calendar is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The access review process is documented alongside the evidence pack held by the owner. The backup rotation is checked against the register of exceptions. The continuity plan is validated by the previous year's assessment. The cloud baseline is measured against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reviewed against the quarterly review notes. The awareness cycle is reconciled with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is evidenced by the agreed service level. The email authentication record is checked against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The third-party register is measured against the previous year's assessment. The privileged access list is measured against the previous year's assessment. The cloud baseline is documented alongside the ticket history for the period. The encryption standard is documented alongside the dependency map. The control is tested at least once every twelve months.

The metric set is reconciled with the most recent exercise record. The classification scheme is documented alongside the previous year's assessment. The classification scheme is measured against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is measured against the dependency map. The vulnerability queue is validated by the quarterly review notes. The hardened build is reviewed against the ticket history for the period. The cloud baseline is reviewed against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is checked against the register of exceptions. The change process is evidenced by the ticket history for the period. The monitoring pipeline is checked against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is documented alongside the signed exception log. The asset register is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is reconciled with the agreed service level. The email authentication record is compared with the previous year's assessment. The vendor register is validated by the most recent exercise record. The threat model is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The mobile standard is measured against the commissioning document. The continuity plan is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

1. The hardened build

The email authentication record is traced to the dependency map. The cloud baseline is reviewed against the ticket history for the period. Any deviation requires written approval and an expiry date.

2. The access review process

The vendor register is evidenced by the dependency map. The remote access path is traced to the agreed service level. The endpoint baseline is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The vendor register is evidenced by the most recent exercise record. The threat model is documented alongside the ticket history for the period. The third-party register is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The third-party register is evidenced by the approved design baseline. The change process is reviewed against the agreed service level. The email authentication record is traced to the dependency map. The procedure is written so a new starter can follow it without supervision.

The threat model is evidenced by the approved design baseline. The mobile standard is validated by the signed exception log. The endpoint baseline is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is checked against the quarterly review notes. The metric set is measured against the agreed service level. The remote access path is reviewed against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The access review process is reviewed against the approved design baseline. The backup rotation is measured against the ticket history for the period. The recovery test is traced to the quarterly review notes. The privileged access list is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is checked against the approved design baseline. The retention schedule is compared with the agreed service level. The access review process is reviewed against the commissioning document. The encryption standard is documented alongside the agreed service level. Metrics are reported as trends rather than single data points.

The backup rotation is reviewed against the approved design baseline. The vulnerability queue is documented alongside the current written standard. The segmentation boundary is documented alongside the approved design baseline. The metric set is reviewed against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The third-party register is compared with the commissioning document. The vendor register is traced to the agreed service level. The encryption standard is documented alongside the evidence pack held by the owner. The vendor register is evidenced by the approved design baseline. Testing covers the failure case, not only the happy path.

Every internet-facing service is validated by the ticket history for the period. The remote access path is compared with the dependency map. The cloud baseline is evidenced by the register of exceptions. The privileged access list is traced to the most recent exercise record. The control is tested at least once every twelve months.

The privileged access list is reviewed against the register of exceptions. The risk register is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is evidenced by the previous year's assessment. The physical controls is validated by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The change process is validated by the approved design baseline. The mobile standard is reconciled with the most recent exercise record. The privileged access list is documented alongside the ticket history for the period. The threat model is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is validated by the quarterly review notes. The monitoring pipeline is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is documented alongside the most recent exercise record. The access review process is checked against the approved design baseline. The backup rotation is compared with the approved design baseline. The access review process is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The vendor register is documented alongside the previous year's assessment. The segmentation boundary is validated by the approved design baseline. The awareness cycle is validated by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is compared with the approved design baseline. The remote access path is compared with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The change process is reconciled with the quarterly review notes. The backup rotation is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The retention schedule is validated by the most recent exercise record. The cloud baseline is evidenced by the current written standard. The control is tested at least once every twelve months.

- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The third-party register is traced to the ticket history for the period. The awareness cycle is validated by the evidence pack held by the owner. The backup rotation is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The classification scheme is checked against the previous year's assessment. The hardened build is reviewed against the commissioning document. The change process is documented alongside the register of exceptions. The encryption standard is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The change process is checked against the previous year's assessment. The privileged access list is compared with the current written standard. The control is tested at least once every twelve months.

The third-party register is traced to the register of exceptions. The encryption standard is traced to the agreed service level. The identity lifecycle is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is documented alongside the dependency map. The metric set is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

- Review date scheduled and visible.
- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

- Notification list confirmed before execution.
- Test result attached to the record.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.

The threat model is checked against the agreed service level. The risk register is measured against the agreed service level. The recovery test is measured against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The patch calendar is reconciled with the most recent exercise record. The threat model is checked against the previous year's assessment. The remote access path is evidenced by the agreed service level. The hardened build is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is documented alongside the signed exception log. The access review process is measured against the previous year's assessment. The risk register is measured against the approved design baseline. The endpoint baseline is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The retention schedule is checked against the current written standard. The recovery test is reconciled with the most recent exercise record. The cloud baseline is reviewed against the current written standard. The mobile standard is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is evidenced by the commissioning document. The awareness cycle is checked against the register of exceptions. The email authentication record is reviewed against the dependency map. The privileged access list is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Test result attached to the record.

The vendor register is checked against the dependency map. Each administrative account is checked against the register of exceptions. Testing covers the failure case, not only the happy path.

The third-party register is traced to the signed exception log. The email authentication record is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The physical controls is evidenced by the approved design baseline. The monitoring pipeline is documented alongside the approved design baseline. The third-party register is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

The vendor register is traced to the commissioning document. The recovery test is reviewed against the agreed service level. The cloud baseline is measured against the approved design baseline. Third parties must demonstrate the control before access is granted.

The metric set is traced to the most recent exercise record. The vulnerability queue is evidenced by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

3. The encryption standard

The retention schedule is documented alongside the commissioning document. The continuity plan is reviewed against the ticket history for the period. The metric set is traced to the evidence pack held by the owner. The vendor register is checked against the most recent exercise record. Testing covers the failure case, not only the happy path.

The access review process is validated by the evidence pack held by the owner. The asset register is compared with the commissioning document. The risk register is reviewed against the commissioning document. The endpoint baseline is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

The patch calendar is checked against the evidence pack held by the owner. The endpoint baseline is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

The privileged access list is reviewed against the most recent exercise record. The continuity plan is compared with the commissioning document. The patch calendar is measured against the ticket history for the period. The classification scheme is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

The encryption standard is documented alongside the approved design baseline. The encryption standard is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The recovery test is checked against the agreed service level. Each administrative account is reconciled with the most recent exercise record. The cloud baseline is documented alongside the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is traced to the ticket history for the period. The asset register is traced to the previous year's assessment. The vulnerability queue is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The classification scheme is validated by the current written standard. The mobile standard is measured against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is reconciled with the approved design baseline. The third-party register is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The segmentation boundary is reconciled with the previous year's assessment. The continuity plan is reviewed against the dependency map. The backup rotation is measured against the commissioning document. The encryption standard is checked against the commissioning document. Any deviation requires written approval and an expiry date.

- Test result attached to the record.
- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.

Every internet-facing service is reviewed against the previous year's assessment. The email authentication record is traced to the ticket history for the period. The email authentication record is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

The vulnerability queue is documented alongside the approved design baseline. The threat model is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is reconciled with the register of exceptions. The classification scheme is measured against the register of exceptions. The privileged access list is measured against the approved design baseline. The vulnerability queue is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The access review process is reconciled with the current written standard. The encryption standard is validated by the approved design baseline. The retention schedule is documented alongside the evidence pack held by the owner. The hardened build is compared with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is traced to the evidence pack held by the owner. The endpoint baseline is documented alongside the current written standard. The continuity plan is evidenced by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The asset register is validated by the evidence pack held by the owner. The cloud baseline is validated by the ticket history for the period. The classification scheme is traced to the register of exceptions. Any deviation requires written approval and an expiry date.

4. The vulnerability queue

The threat model is checked against the evidence pack held by the owner. The change process is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

The asset register is compared with the current written standard. The access review process is traced to the evidence pack held by the owner. Every internet-facing service is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

The risk register is compared with the most recent exercise record. The access review process is evidenced by the ticket history for the period. The mobile standard is checked against the agreed service level. The asset register is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The metric set is validated by the previous year's assessment. The threat model is checked against the agreed service level. Each administrative account is measured against the previous year's assessment. Testing covers the failure case, not only the happy path.

The vulnerability queue is reviewed against the previous year's assessment. The patch calendar is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The endpoint baseline is documented alongside the previous year's assessment. The metric set is compared with the evidence pack held by the owner. The metric set is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The email authentication record is reconciled with the signed exception log. The email authentication record is measured against the most recent exercise record. The risk register is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the register of exceptions. The physical controls is compared with the quarterly review notes. The asset register is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is traced to the current written standard. The identity lifecycle is compared with the signed exception log. The patch calendar is compared with the commissioning document. The endpoint baseline is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is validated by the current written standard. The vendor register is traced to the register of exceptions. The backup rotation is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

5. The continuity plan

The email authentication record is checked against the approved design baseline. The physical controls is measured against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The asset register is documented alongside the ticket history for the period. The physical controls is reviewed against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is documented alongside the signed exception log. The endpoint baseline is reconciled with the dependency map. Every internet-facing service is documented alongside the current written standard. The continuity plan is documented alongside the ticket history for the period. Metrics are reported as trends rather than single data points.

The remote access path is traced to the current written standard. The vendor register is documented alongside the most recent exercise record. The physical controls is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is traced to the approved design baseline. The physical controls is compared with the evidence pack held by the owner. The segmentation boundary is measured against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vendor register is evidenced by the quarterly review notes. The encryption standard is traced to the register of exceptions. The control is tested at least once every twelve months.

The hardened build is documented alongside the dependency map. The change process is compared with the dependency map. The change process is reviewed against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Test result attached to the record.
- Exception route documented and time-bound.

The identity lifecycle is compared with the most recent exercise record. The retention schedule is checked against the most recent exercise record. The threat model is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is documented alongside the register of exceptions. The patch calendar is evidenced by the commissioning document. The vulnerability queue is evidenced by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The threat model is validated by the register of exceptions. The asset register is documented alongside the commissioning document. The access review process is traced to the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The physical controls is measured against the most recent exercise record. The continuity plan is reconciled with the agreed service level. The asset register is traced to the commissioning document. The encryption standard is reviewed against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The threat model is reconciled with the approved design baseline. The privileged access list is reviewed against the evidence pack held by the owner. The remote access path is reconciled with the commissioning document. Records are retained only as long as the schedule requires.

The risk register is documented alongside the evidence pack held by the owner. The retention schedule is checked against the quarterly review notes. The encryption standard is traced to the signed exception log. Testing covers the failure case, not only the happy path.

The hardened build is validated by the most recent exercise record. The threat model is reconciled with the agreed service level. The patch calendar is validated by the commissioning document. The third-party register is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

The identity lifecycle is validated by the dependency map. The patch calendar is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the quarterly review notes. The patch calendar is reviewed against the agreed service level. The continuity plan is documented alongside the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is compared with the evidence pack held by the owner. The identity lifecycle is evidenced by the previous year's assessment. The encryption standard is reviewed against the dependency map. The privileged access list is compared with the quarterly review notes. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.

The hardened build is validated by the agreed service level. The threat model is checked against the signed exception log. The endpoint baseline is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

6. The cloud baseline

The vendor register is compared with the quarterly review notes. Each administrative account is reconciled with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is validated by the signed exception log. The remote access path is compared with the commissioning document. The patch calendar is traced to the agreed service level. Third parties must demonstrate the control before access is granted.

Each administrative account is compared with the previous year's assessment. The identity lifecycle is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is evidenced by the most recent exercise record. The cloud baseline is measured against the commissioning document. Each administrative account is measured against the previous year's assessment. The remote access path is traced to the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is validated by the dependency map. The change process is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The segmentation boundary is documented alongside the agreed service level. The vendor register is compared with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is compared with the register of exceptions. The awareness cycle is validated by the quarterly review notes. Every internet-facing service is documented alongside the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is reviewed against the commissioning document. The physical controls is validated by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is reconciled with the register of exceptions. The physical controls is validated by the signed exception log. The retention schedule is checked against the approved design baseline. The awareness cycle is reviewed against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reviewed against the quarterly review notes. Every internet-facing service is evidenced by the approved design baseline. The continuity plan is checked against the approved design baseline. The remote access path is measured against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The continuity plan is traced to the dependency map. Each administrative account is checked against the commissioning document. The continuity plan is evidenced by the agreed service level. The hardened build is compared with the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is documented alongside the ticket history for the period. The hardened build is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

Every internet-facing service is documented alongside the quarterly review notes. The segmentation boundary is compared with the agreed service level. The cloud baseline is validated by the dependency map. The recovery test is traced to the signed exception log. The procedure is written so a new starter can follow it without supervision.