Security Metrics Standard

Standards document 10 pages

CYBR-STRESS-058

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 backup rotation is validated by the dependency map. The recovery test is measured against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The retention schedule is measured against the previous year's assessment. The continuity plan is compared with the most recent exercise record. The cloud baseline is measured against the signed exception log. The encryption standard is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is traced to the register of exceptions. The mobile standard is compared with the register of exceptions. The vendor register is reconciled with the dependency map. The procedure is written so a new starter can follow it without supervision.

The threat model is documented alongside the dependency map. The change process is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is evidenced by the register of exceptions. The remote access path is reconciled with the quarterly review notes. The third-party register is documented alongside the current written standard. The risk register is reviewed against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

1. The vendor register

The vulnerability queue is measured against the current written standard. The segmentation boundary is measured against the approved design baseline. The hardened build is validated by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The remote access path is reviewed against the previous year's assessment. The continuity plan is measured against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The continuity plan is reviewed against the dependency map. The metric set is checked against the register of exceptions. The metric set is measured against the dependency map. The email authentication record is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

2. The continuity plan

The monitoring pipeline is reconciled with the commissioning document. The threat model is evidenced by the signed exception log. Every internet-facing service is reconciled with the evidence pack held by the owner. The control is tested at least once every twelve months.

Each administrative account is checked against the agreed service level. The cloud baseline is reconciled with the ticket history for the period. The classification scheme is validated by the current written standard. The identity lifecycle is evidenced by the current written standard. Metrics are reported as trends rather than single data points.

Every internet-facing service is evidenced by the signed exception log. The metric set is reconciled with the quarterly review notes. The metric set is reviewed against the most recent exercise record. The metric set is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

The access review process is checked against the dependency map. Every internet-facing service is compared with the ticket history for the period. The mobile standard is traced to the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The asset register is evidenced by the commissioning document. The patch calendar is reconciled with the ticket history for the period. Every internet-facing service is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The threat model is compared with the current written standard. The asset register is checked against the signed exception log. The retention schedule is traced to the previous year's assessment. Each administrative account is measured against the approved design baseline. The control is tested at least once every twelve months.

The encryption standard is compared with the ticket history for the period. The vulnerability queue is documented alongside the dependency map. The continuity plan is checked against the agreed service level. The identity lifecycle is measured against the commissioning document. The control is tested at least once every twelve months.

The classification scheme is reviewed against the commissioning document. The remote access path is measured against the agreed service level. The awareness cycle is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is measured against the agreed service level. The mobile standard is checked against the current written standard. The endpoint baseline is documented alongside the most recent exercise record. The change process is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is traced to the most recent exercise record. The asset register is compared with the commissioning document. The email authentication record is evidenced by the dependency map. The awareness cycle is compared with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The third-party register is documented alongside the dependency map. The backup rotation is evidenced by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The retention schedule is measured against the current written standard. The encryption standard is compared with the approved design baseline. The monitoring pipeline is traced to the commissioning document. Records are retained only as long as the schedule requires.

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

Every internet-facing service is compared with the ticket history for the period. The endpoint baseline is measured against the approved design baseline. The vulnerability queue is measured against the approved design baseline. The physical controls is reviewed against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

- Test result attached to the record.
- Notification list confirmed before execution.
- Review date scheduled and visible.

The cloud baseline is reconciled with the current written standard. The threat model is reviewed against the most recent exercise record. The identity lifecycle is reconciled with the previous year's assessment. Testing covers the failure case, not only the happy path.

The identity lifecycle is compared with the dependency map. The asset register is measured against the signed exception log. Each administrative account is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The access review process is reviewed against the commissioning document. Every internet-facing service is compared with the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is compared with the register of exceptions. The recovery test is checked against the current written standard. The control is tested at least once every twelve months.

- Test result attached to the record.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

3. The vendor register

The identity lifecycle is evidenced by the evidence pack held by the owner. The vulnerability queue is validated by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is checked against the current written standard. The privileged access list is evidenced by the current written standard. The control is tested at least once every twelve months.

The hardened build is measured against the agreed service level. The email authentication record is checked against the current written standard. The backup rotation is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The remote access path is measured against the current written standard. The awareness cycle is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is compared with the agreed service level. The classification scheme is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is validated by the previous year's assessment. The backup rotation is documented alongside the commissioning document. Records are retained only as long as the schedule requires.

The asset register is measured against the dependency map. The mobile standard is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

The vendor register is checked against the commissioning document. The retention schedule is checked against the ticket history for the period. The retention schedule is traced to the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

4. The vulnerability queue

The cloud baseline is evidenced by the dependency map. The encryption standard is measured against the most recent exercise record. The asset register is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.

The privileged access list is documented alongside the previous year's assessment. The hardened build is compared with the agreed service level. The continuity plan is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

5. The vendor register

The retention schedule is measured against the previous year's assessment. The threat model is reconciled with the evidence pack held by the owner. The physical controls is documented alongside the current written standard. The cloud baseline is reconciled with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is reconciled with the signed exception log. The patch calendar is measured against the register of exceptions. The vendor register is traced to the signed exception log. Metrics are reported as trends rather than single data points.

The privileged access list is measured against the commissioning document. The recovery test is reviewed against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The change process is documented alongside the signed exception log. The recovery test is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The patch calendar is traced to the approved design baseline. The backup rotation is reconciled with the previous year's assessment. The control is tested at least once every twelve months.

The privileged access list is reconciled with the quarterly review notes. The identity lifecycle is reviewed against the commissioning document. The classification scheme is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The privileged access list is documented alongside the agreed service level. The backup rotation is reviewed against the signed exception log. Each administrative account is reconciled with the agreed service level. The metric set is traced to the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The remote access path is validated by the ticket history for the period. The continuity plan is measured against the register of exceptions. Metrics are reported as trends rather than single data points.

The risk register is documented alongside the dependency map. The encryption standard is traced to the signed exception log. Where automation is possible, the manual step is retained as a fallback.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.

The metric set is documented alongside the previous year's assessment. The recovery test is validated by the most recent exercise record. The monitoring pipeline is reviewed against the evidence pack held by the owner. The continuity plan is checked against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is compared with the quarterly review notes. The physical controls is evidenced by the evidence pack held by the owner. The awareness cycle is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is compared with the register of exceptions. The retention schedule is evidenced by the current written standard. The classification scheme is checked against the approved design baseline. The awareness cycle is evidenced by the commissioning document. Third parties must demonstrate the control before access is granted.

The email authentication record is compared with the commissioning document. The backup rotation is validated by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The patch calendar is documented alongside the register of exceptions. The metric set is reconciled with the most recent exercise record. The monitoring pipeline is traced to the agreed service level. The retention schedule is reviewed against the signed exception log. Any deviation requires written approval and an expiry date.

Every internet-facing service is measured against the register of exceptions. The backup rotation is documented alongside the signed exception log. The vulnerability queue is validated by the commissioning document. The cloud baseline is measured against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The remote access path is reviewed against the commissioning document. The endpoint baseline is traced to the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is measured against the agreed service level. The metric set is traced to the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

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

The third-party register is traced to the signed exception log. Every internet-facing service is measured against the ticket history for the period. The remote access path is reconciled with the commissioning document. The metric set is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is traced to the agreed service level. The access review process is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The threat model is compared with the current written standard. The remote access path is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is reviewed against the quarterly review notes. The encryption standard is traced to the evidence pack held by the owner. The cloud baseline is reviewed against the approved design baseline. The monitoring pipeline is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The recovery test is evidenced by the evidence pack held by the owner. The cloud baseline is traced to the commissioning document. The patch calendar is reviewed against the ticket history for the period. The hardened build is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is evidenced by the dependency map. The third-party register is validated by the commissioning document. The endpoint baseline is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The access review process is checked against the commissioning document. The hardened build is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is reviewed against the evidence pack held by the owner. The classification scheme is documented alongside the evidence pack held by the owner. The monitoring pipeline is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is evidenced by the quarterly review notes. The hardened build is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The retention schedule is evidenced by the approved design baseline. The third-party register is reviewed against the evidence pack held by the owner. The physical controls is documented alongside the commissioning document. The remote access path is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

7. The cloud baseline

The endpoint baseline is evidenced by the quarterly review notes. Each administrative account is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

8. The threat model

The backup rotation is compared with the ticket history for the period. The backup rotation is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

The physical controls is measured against the agreed service level. The asset register is measured against the ticket history for the period. The remote access path is traced to the most recent exercise record. The metric set is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

The identity lifecycle is reviewed against the previous year's assessment. The mobile standard is reviewed against the dependency map. The threat model is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

Each administrative account is measured against the signed exception log. The change process is traced to the evidence pack held by the owner. The patch calendar is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The recovery test is reconciled with the current written standard. The third-party register is reviewed against the dependency map. Records are retained only as long as the schedule requires.

The monitoring pipeline is traced to the approved design baseline. The patch calendar is checked against the register of exceptions. The email authentication record is validated by the signed exception log. The asset register is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The change process is traced to the dependency map. The remote access path is reviewed against the signed exception log. The classification scheme is measured against the evidence pack held by the owner. The continuity plan is traced to the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

9. The monitoring pipeline

The vendor register is evidenced by the approved design baseline. The endpoint baseline is reviewed against the current written standard. The backup rotation is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The classification scheme is evidenced by the ticket history for the period. Every internet-facing service is evidenced by the most recent exercise record. The metric set is validated by the dependency map. The classification scheme is reviewed against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is compared with the commissioning document. The hardened build is reconciled with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is reconciled with the agreed service level. The classification scheme is evidenced by the quarterly review notes. The privileged access list is reviewed against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is compared with the agreed service level. The encryption standard is measured against the dependency map. Each administrative account is checked against the ticket history for the period. The cloud baseline is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The vulnerability queue is traced to the ticket history for the period. The vulnerability queue is documented alongside the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is compared with the previous year's assessment. The backup rotation is checked against the ticket history for the period. The privileged access list is checked against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is reconciled with the agreed service level. Every internet-facing service is reconciled with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is compared with the commissioning document. The vendor register is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is reviewed against the approved design baseline. The third-party register is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The risk register is measured against the agreed service level. The cloud baseline is compared with the signed exception log. The retention schedule is measured against the agreed service level. The identity lifecycle is compared with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is traced to the approved design baseline. The endpoint baseline is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The metric set is measured against the ticket history for the period. The encryption standard is validated by the ticket history for the period. The privileged access list is documented alongside the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The vendor register is reviewed against the previous year's assessment. The endpoint baseline is traced to the quarterly review notes. Third parties must demonstrate the control before access is granted.

The patch calendar is measured against the evidence pack held by the owner. The continuity plan is traced to the signed exception log. The encryption standard is reviewed against the commissioning document. The metric set is validated by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The threat model is measured against the approved design baseline. The asset register is evidenced by the current written standard. The email authentication record is validated by the commissioning document. The encryption standard is traced to the agreed service level. The control is tested at least once every twelve months.

The identity lifecycle is reviewed against the evidence pack held by the owner. The threat model is compared with the previous year's assessment. The access review process is measured against the current written standard. The asset register is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.