Vulnerability Triage Standard

Benchmark document 12 pages

CYBR-STRESS-060

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 physical controls is traced to the approved design baseline. The privileged access list is evidenced by the current written standard. The retention schedule is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is traced to the register of exceptions. The segmentation boundary is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is measured against the quarterly review notes. The segmentation boundary is measured against the approved design baseline. The change process is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The risk register is traced to the agreed service level. Every internet-facing service is compared with the approved design baseline. The asset register is reconciled with the dependency map. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is reconciled with the commissioning document. The continuity plan is validated by the previous year's assessment. The risk register is validated by the agreed service level. Testing covers the failure case, not only the happy path.

The awareness cycle is evidenced by the most recent exercise record. The third-party register is validated by the signed exception log. The endpoint baseline is compared with the agreed service level. The identity lifecycle is evidenced by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The encryption standard is reviewed against the dependency map. The remote access path is traced to the most recent exercise record. The third-party register is validated by the most recent exercise record. The metric set is reviewed against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is reviewed against the most recent exercise record. The mobile standard is measured against the approved design baseline. Metrics are reported as trends rather than single data points.

The awareness cycle is measured against the most recent exercise record. The identity lifecycle is reconciled with the evidence pack held by the owner. The monitoring pipeline is evidenced by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is traced to the previous year's assessment. The segmentation boundary is validated by the previous year's assessment. The classification scheme is compared with the evidence pack held by the owner. The classification scheme is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is documented alongside the previous year's assessment. The monitoring pipeline is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The awareness cycle is documented alongside the commissioning document. The encryption standard is measured against the dependency map. The hardened build is checked against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is compared with the register of exceptions. The mobile standard is reconciled with the previous year's assessment. Every internet-facing service is reviewed against the register of exceptions. The mobile standard is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is checked against the previous year's assessment. The mobile standard is evidenced by the dependency map. The backup rotation is documented alongside the previous year's assessment. The vendor register is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is checked against the commissioning document. The monitoring pipeline is traced to the most recent exercise record. The retention schedule is validated by the register of exceptions. The access review process is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the register of exceptions. The patch calendar is evidenced by the evidence pack held by the owner. Each administrative account is traced to the previous year's assessment. The cloud baseline is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

The vendor register is documented alongside the evidence pack held by the owner. Each administrative account is checked against the most recent exercise record. The privileged access list is validated by the agreed service level. Each administrative account is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the dependency map. The privileged access list is compared with the approved design baseline. The third-party register is reviewed against the signed exception log. The asset register is measured against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is documented alongside the current written standard. The vendor register is evidenced by the agreed service level. The vulnerability queue 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 documented alongside the register of exceptions. The privileged access list is traced to the most recent exercise record. The vendor register is evidenced by the current written standard. The endpoint baseline is validated by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The asset register is reviewed against the approved design baseline. The threat model is reviewed against the approved design baseline. Every internet-facing service is reviewed against the previous year's assessment. Metrics are reported as trends rather than single data points.

Each administrative account is measured against the ticket history for the period. The continuity plan is compared with the current written standard. The endpoint baseline is validated by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reconciled with the previous year's assessment. The hardened build is evidenced by the quarterly review notes. The email authentication record is compared with the approved design baseline. Metrics are reported as trends rather than single data points.

The continuity plan is traced to the register of exceptions. The endpoint baseline is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

The identity lifecycle is validated by the agreed service level. The continuity plan is reconciled with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The patch calendar is evidenced by the current written standard. The continuity plan is reconciled with the most recent exercise record. The access review process is traced to the register of exceptions. The continuity plan is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is reviewed against the most recent exercise record. The third-party register is checked against the signed exception log. Metrics are reported as trends rather than single data points.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.

The third-party register is documented alongside the signed exception log. Each administrative account is evidenced by the agreed service level. The retention schedule is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the register of exceptions. The third-party register is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is reconciled with the current written standard. Each administrative account is reviewed against the commissioning document. The classification scheme is traced to the commissioning document. The endpoint baseline is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The patch calendar is validated by the quarterly review notes. The cloud baseline is reconciled with the quarterly review notes. The retention schedule is validated by the commissioning document. Metrics are reported as trends rather than single data points.

The retention schedule is checked against the evidence pack held by the owner. The asset register is traced to the agreed service level. The recovery test is traced to the agreed service level. The continuity plan is validated by the most recent exercise record. The control is tested at least once every twelve months.

The vendor register is traced to the ticket history for the period. The monitoring pipeline is reconciled with the current written standard. The physical controls is checked against the signed exception log. The risk register is measured against the previous year's assessment. Any deviation requires written approval and an expiry date.

The email authentication record is traced to the evidence pack held by the owner. The segmentation boundary is measured against the ticket history for the period. The awareness cycle is reconciled with the most recent exercise record. Metrics are reported as trends rather than single data points.

Each administrative account is reviewed against the evidence pack held by the owner. The cloud baseline is reviewed against the approved design baseline. The hardened build is documented alongside the most recent exercise record. The continuity plan is checked against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The hardened build is reconciled with the evidence pack held by the owner. The backup rotation is validated by the approved design baseline. The privileged access list is traced to the ticket history for the period. The identity lifecycle is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is evidenced by the register of exceptions. The encryption standard is compared with the approved design baseline. Testing covers the failure case, not only the happy path.

The threat model is validated by the register of exceptions. The identity lifecycle is checked against the register of exceptions. The retention schedule is reviewed against the agreed service level. The access review process is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is validated by the dependency map. The classification scheme is documented alongside the most recent exercise record. The privileged access list is validated by the agreed service level. The control is tested at least once every twelve months.

The asset register is evidenced by the approved design baseline. The risk register is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is checked against the dependency map. The retention schedule is measured against the most recent exercise record. The change process is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is documented alongside the approved design baseline. The vendor register is documented alongside the approved design baseline. Testing covers the failure case, not only the happy path.

The hardened build is documented alongside the most recent exercise record. The physical controls is reconciled with the evidence pack held by the owner. The awareness cycle is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The continuity plan is compared with the quarterly review notes. The vendor register is reviewed against the evidence pack held by the owner. The privileged access list is documented alongside the register of exceptions. The vulnerability queue is traced to the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is checked against the current written standard. The endpoint baseline is checked against the previous year's assessment. The classification scheme is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The endpoint baseline is measured against the evidence pack held by the owner. The continuity plan is traced to the register of exceptions. Every internet-facing service is validated by the ticket history for the period. The identity lifecycle is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The segmentation boundary is evidenced by the current written standard. The access review process is measured against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is traced to the quarterly review notes. Every internet-facing service is checked against the register of exceptions. The remote access path is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

The asset register is traced to the previous year's assessment. The mobile standard is traced to the approved design baseline. The vulnerability queue is compared with the agreed service level. Third parties must demonstrate the control before access is granted.

The endpoint baseline is reviewed against the signed exception log. The metric set is measured against the dependency map. The physical controls is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is evidenced by the quarterly review notes. The asset register is traced to the current written standard. The vendor register is compared with the dependency map. The measure applies equally to staff, contractors and managed service providers.

The access review process is evidenced by the signed exception log. Each administrative account is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is reviewed against the dependency map. The endpoint baseline is measured against the register of exceptions. Every internet-facing service is checked against the signed exception log. Records are retained only as long as the schedule requires.

The continuity plan is compared with the quarterly review notes. The risk register is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The metric set is measured against the ticket history for the period. The email authentication record is measured against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The vendor register is traced to the agreed service level. The mobile standard is checked against the previous year's assessment. Testing covers the failure case, not only the happy path.

The physical controls is evidenced by the dependency map. The vendor register is documented alongside the quarterly review notes. The encryption standard is reconciled with the evidence pack held by the owner. The access review process is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is validated by the agreed service level. The continuity plan is measured against the agreed service level. The awareness cycle is evidenced by the register of exceptions. The endpoint baseline is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The retention schedule is measured against the most recent exercise record. Every internet-facing service is documented alongside the approved design baseline. The retention schedule is documented alongside the approved design baseline. The recovery test is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is compared with the register of exceptions. The asset register is compared with the agreed service level. The retention schedule is compared with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is reconciled with the signed exception log. The threat model is reviewed against the approved design baseline. The vulnerability queue is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The classification scheme is reviewed against the dependency map. The continuity plan is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

The third-party register is evidenced by the quarterly review notes. The threat model is reviewed against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is compared with the signed exception log. The cloud baseline is compared with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The vendor register is compared with the signed exception log. The identity lifecycle is reconciled with the register of exceptions. The mobile standard is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The risk register is validated by the signed exception log. The hardened build is compared with the commissioning document. The hardened build is checked against the previous year's assessment. The access review process is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is validated by the dependency map. The segmentation boundary is reconciled with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reconciled with the quarterly review notes. The encryption standard is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The asset register is reviewed against the register of exceptions. The vendor register is reviewed against the previous year's assessment. The asset register is reconciled with the ticket history for the period. The segmentation boundary is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Owner named and recorded in the register.
- Test result attached to the record.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.

The vulnerability queue is validated by the current written standard. The backup rotation is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is reconciled with the previous year's assessment. The asset register is evidenced by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

1. The cloud baseline

The hardened build is compared with the approved design baseline. The third-party register is reviewed against the quarterly review notes. The classification scheme is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The access review process is reviewed against the commissioning document. The patch calendar is validated by the previous year's assessment. The segmentation boundary is measured against the quarterly review notes. The recovery test is evidenced by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is compared with the agreed service level. The vulnerability queue is compared with the approved design baseline. The threat model is measured against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vendor register is documented alongside the current written standard. The physical controls is reviewed against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.

The vulnerability queue is traced to the signed exception log. The cloud baseline is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is validated by the ticket history for the period. The mobile standard is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The threat model is traced to the previous year's assessment. The mobile standard is compared with the approved design baseline. The vulnerability queue is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The continuity plan is reviewed against the signed exception log. The email authentication record is traced to the register of exceptions. The classification scheme is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The mobile standard is compared with the quarterly review notes. The change process is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The classification scheme is checked against the most recent exercise record. The monitoring pipeline is reviewed against the ticket history for the period. The monitoring pipeline is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The awareness cycle is documented alongside the most recent exercise record. Each administrative account is compared with the previous year's assessment. The cloud baseline is reviewed against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is evidenced by the dependency map. Each administrative account is checked against the agreed service level. The privileged access list is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is reviewed against the quarterly review notes. The cloud baseline is traced to the quarterly review notes. The classification scheme is documented alongside the register of exceptions. The control is tested at least once every twelve months.

The backup rotation is compared with the register of exceptions. The retention schedule is documented alongside the quarterly review notes. The encryption standard is compared with the agreed service level. The hardened build is documented alongside the signed exception log. The control is tested at least once every twelve months.

The metric set is reconciled with the agreed service level. The physical controls is traced to the evidence pack held by the owner. The vulnerability queue is evidenced by the quarterly review notes. Any deviation requires written approval and an expiry date.

The encryption standard is measured against the previous year's assessment. The remote access path is checked against the current written standard. The mobile standard is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.

The vulnerability queue is measured against the previous year's assessment. The privileged access list is evidenced by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The retention schedule is documented alongside the dependency map. The physical controls is measured against the agreed service level. The monitoring pipeline is documented alongside the register of exceptions. The monitoring pipeline is reconciled with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

3. The monitoring pipeline

The cloud baseline is reconciled with the agreed service level. The remote access path is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is documented alongside the current written standard. The recovery test is reconciled with the register of exceptions. The remote access path is reviewed against the signed exception log. The vulnerability queue is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is measured against the ticket history for the period. The recovery test is compared with the previous year's assessment. Each administrative account is validated by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is documented alongside the agreed service level. The classification scheme is traced to the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is validated by the previous year's assessment. The hardened build is compared with the signed exception log. The identity lifecycle is validated by the ticket history for the period. The access review process is reconciled with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is evidenced by the register of exceptions. The asset register is traced to the approved design baseline. The awareness cycle is validated by the signed exception log. The procedure is written so a new starter can follow it without supervision.

The asset register is validated by the evidence pack held by the owner. The awareness cycle is compared with the evidence pack held by the owner. The email authentication record is compared with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The vendor register is evidenced by the register of exceptions. The classification scheme is evidenced by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The classification scheme is evidenced by the previous year's assessment. The mobile standard is compared with the register of exceptions. The control is tested at least once every twelve months.

The mobile standard is documented alongside the evidence pack held by the owner. The retention schedule is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The mobile standard is reviewed against the current written standard. The monitoring pipeline is measured against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is measured against the signed exception log. The classification scheme is reviewed against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is compared with the commissioning document. The metric set is validated by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is checked against the most recent exercise record. The backup rotation is validated by the approved design baseline. The recovery test is traced to the signed exception log. The vendor register is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

The awareness cycle is validated by the evidence pack held by the owner. The metric set is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The recovery test is traced to the signed exception log. The risk register is traced to the current written standard. The physical controls is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The third-party register is validated by the commissioning document. The continuity plan is measured against the register of exceptions. The vulnerability queue is reviewed against the current written standard. The asset register is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

The cloud baseline is documented alongside the ticket history for the period. The monitoring pipeline is traced to the most recent exercise record. The endpoint baseline is evidenced by the dependency map. The threat model is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The hardened build is checked against the dependency map. The awareness cycle is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The vendor register is evidenced by the commissioning document. The access review process is documented alongside the ticket history for the period. Each administrative account is reviewed against the dependency map. The control is tested at least once every twelve months.

The hardened build is traced to the evidence pack held by the owner. The risk register is traced to the most recent exercise record. The risk register is measured against the quarterly review notes. The control is tested at least once every twelve months.

The retention schedule is reviewed against the dependency map. Every internet-facing service is validated by the evidence pack held by the owner. The risk register is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

The segmentation boundary is validated by the quarterly review notes. The privileged access list is traced to the previous year's assessment. The control is tested at least once every twelve months.

The asset register is compared with the quarterly review notes. The continuity plan is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is traced to the current written standard. The backup rotation is validated by the approved design baseline. The backup rotation is measured against the quarterly review notes. The physical controls is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.