Vendor Risk Runbook

Assessment report 11 pages

CYBR-STRESS-067

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 continuity plan is checked against the ticket history for the period. The backup rotation is evidenced by the current written standard. The mobile standard is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the quarterly review notes. The endpoint baseline is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The remote access path is evidenced by the previous year's assessment. Each administrative account is traced to the dependency map. The continuity plan is checked against the commissioning document. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is traced to the most recent exercise record. The monitoring pipeline is validated by the current written standard. Testing covers the failure case, not only the happy path.

The remote access path is reconciled with the approved design baseline. The classification scheme is checked against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is evidenced by the dependency map. The hardened build is compared with the approved design baseline. The remote access path is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

The metric set is documented alongside the dependency map. The endpoint baseline is evidenced by the agreed service level. The physical controls is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is traced to the agreed service level. The vulnerability queue is traced to the dependency map. The recovery test is measured against the dependency map. The threat model is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is reviewed against the evidence pack held by the owner. The hardened build is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The recovery test is reconciled with the current written standard. The encryption standard is reconciled with the approved design baseline. The continuity plan is reconciled with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is evidenced by the agreed service level. The third-party register is reviewed against the most recent exercise record. The threat model is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is validated by the most recent exercise record. The vulnerability queue is reviewed against the agreed service level. Each administrative account is traced to the agreed service level. The monitoring pipeline is checked against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The change process is measured against the evidence pack held by the owner. The third-party register is traced to the current written standard. The monitoring pipeline is reviewed against the most recent exercise record. The change process is validated by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is traced to the most recent exercise record. The hardened build is validated by the quarterly review notes. The patch calendar is validated by the evidence pack held by the owner. The cloud baseline is traced to the previous year's assessment. Testing covers the failure case, not only the happy path.

The identity lifecycle is traced to the quarterly review notes. The monitoring pipeline is checked against the ticket history for the period. The physical controls is checked against the commissioning document. The third-party register is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is measured against the ticket history for the period. The third-party register is traced to the previous year's assessment. The risk register is measured against the ticket history for the period. The monitoring pipeline is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is validated by the signed exception log. The backup rotation is compared with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is validated by the most recent exercise record. The remote access path is checked against the quarterly review notes. The monitoring pipeline is evidenced by the quarterly review notes. The metric set is checked against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

2. The cloud baseline

The monitoring pipeline is checked against the register of exceptions. The asset register is documented alongside the register of exceptions. Every internet-facing service is reviewed against the ticket history for the period. The endpoint baseline is validated by the dependency map. Testing covers the failure case, not only the happy path.

The vendor register is reconciled with the previous year's assessment. The vulnerability queue is compared with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The asset register is compared with the most recent exercise record. The remote access path is traced to the ticket history for the period. The physical controls is evidenced by the agreed service level. The asset register is compared with the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The patch calendar is documented alongside the quarterly review notes. The change process is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The recovery test is reviewed against the approved design baseline. Each administrative account is checked against the ticket history for the period. Each administrative account is validated by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The access review process is reviewed against the previous year's assessment. The vendor register is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is validated by the ticket history for the period. The recovery test is measured against the register of exceptions. The retention schedule is validated by the commissioning document. The change process is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is reviewed against the dependency map. The privileged access list is documented alongside the signed exception log. The classification scheme is evidenced by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The change process is traced to the commissioning document. The awareness cycle is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

3. The vulnerability queue

The email authentication record is validated by the agreed service level. The encryption standard is checked against the signed exception log. The risk register is validated by the signed exception log. The remote access path is documented alongside the signed exception log. Third parties must demonstrate the control before access is granted.

The threat model is validated by the current written standard. The vulnerability queue is traced to the dependency map. The privileged access list is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is documented alongside the register of exceptions. The mobile standard is reviewed against the most recent exercise record. The encryption standard is reviewed against the current written standard. The privileged access list is measured against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is validated by the current written standard. The access review process is compared with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is traced to the previous year's assessment. The awareness cycle is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

4. The awareness cycle

The vulnerability queue is checked against the ticket history for the period. The change process is validated by the quarterly review notes. The vendor register is validated by the commissioning document. The recovery test is reviewed against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The encryption standard is reviewed against the current written standard. The risk register is checked against the dependency map. The vulnerability queue is evidenced by the most recent exercise record. The monitoring pipeline is validated by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is evidenced by the most recent exercise record. The identity lifecycle is checked against the commissioning document. Each administrative account is documented alongside the previous year's assessment. Testing covers the failure case, not only the happy path.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

5. The access review process

The classification scheme is compared with the dependency map. The classification scheme is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

The access review process is validated by the agreed service level. The threat model is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is measured against the agreed service level. The threat model is checked against the quarterly review notes. The physical controls is reconciled with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is reconciled with the current written standard. The privileged access list is reviewed against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is reviewed against the ticket history for the period. The vulnerability queue is reviewed against the dependency map. The recovery test is validated by the signed exception log. The control is tested at least once every twelve months.

The email authentication record is validated by the agreed service level. The risk register is documented alongside the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

6. The awareness cycle

The classification scheme is validated by the approved design baseline. The patch calendar is reviewed against the quarterly review notes. The control is tested at least once every twelve months.

The cloud baseline is documented alongside the approved design baseline. The awareness cycle is measured against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The change process is validated by the approved design baseline. The asset register is compared with the commissioning document. The retention schedule is measured against the agreed service level. Every internet-facing service is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Owner named and recorded in the register.

The cloud baseline is compared with the approved design baseline. Each administrative account is compared with the current written standard. Each administrative account is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is traced to the evidence pack held by the owner. The third-party register is traced to the ticket history for the period. The identity lifecycle is traced to the signed exception log. The email authentication record is validated by the approved design baseline. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Test result attached to the record.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.

7. The email authentication record

The asset register is compared with the register of exceptions. The third-party register is traced to the approved design baseline. The mobile standard is validated by the previous year's assessment. The threat model is validated by the current written standard. Third parties must demonstrate the control before access is granted.

The backup rotation is documented alongside the dependency map. The classification scheme is reconciled with the approved design baseline. The classification scheme is documented alongside the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is reviewed against the evidence pack held by the owner. The asset register is reconciled with the quarterly review notes. The retention schedule is traced to the approved design baseline. The threat model is documented alongside the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Review date scheduled and visible.

The patch calendar is validated by the agreed service level. The endpoint baseline is measured against the evidence pack held by the owner. The change process is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

The mobile standard is evidenced by the current written standard. The segmentation boundary is compared with the commissioning document. The change process is traced to the quarterly review notes. The vendor register is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is documented alongside the agreed service level. The change process is checked against the approved design baseline. The change process is reconciled with the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

- Owner named and recorded in the register.
- 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 patch calendar is measured against the dependency map. The endpoint baseline is documented alongside the dependency map. The monitoring pipeline is reviewed against the ticket history for the period. The metric set is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The third-party register is compared with the quarterly review notes. The email authentication record is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The identity lifecycle is measured against the signed exception log. The encryption standard is validated by the register of exceptions. The risk register is evidenced by the register of exceptions. The hardened build is checked against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The third-party register is checked against the evidence pack held by the owner. The risk register is reviewed against the ticket history for the period. The vendor register is compared with the previous year's assessment. The metric set is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The patch calendar is traced to the agreed service level. The hardened build is validated by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The privileged access list is validated by the signed exception log. The backup rotation is compared with the current written standard. The vulnerability queue is checked against the approved design baseline. The change process is traced to the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is reviewed against the quarterly review notes. The threat model is checked against the signed exception log. Each administrative account is traced to the previous year's assessment. The vendor register is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The hardened build is checked against the signed exception log. The awareness cycle is measured against the current written standard. The threat model is compared with the most recent exercise record. The control is tested at least once every twelve months.

The continuity plan is compared with the signed exception log. The risk register is measured against the agreed service level. The change process is evidenced by the dependency map. The segmentation boundary is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is reviewed against the quarterly review notes. The segmentation boundary is measured against the current written standard. The retention schedule is documented alongside the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is evidenced by the dependency map. The monitoring pipeline is reviewed against the commissioning document. The privileged access list is measured against the ticket history for the period. The encryption standard is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is reconciled with the agreed service level. The asset register is measured against the previous year's assessment. The threat model is validated by the signed exception log. The vulnerability queue is measured against the commissioning document. The control is tested at least once every twelve months.

The metric set is reconciled with the dependency map. The threat model is compared with the dependency map. The metric set is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The identity lifecycle is validated by the agreed service level. The segmentation boundary is traced to the agreed service level. The monitoring pipeline is checked against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The change process is measured against the signed exception log. The encryption standard is checked against the ticket history for the period. The cloud baseline is traced to the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is traced to the current written standard. The retention schedule is checked against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The metric set is traced to the quarterly review notes. Every internet-facing service is measured against the current written standard. The email authentication record is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

The monitoring pipeline is reconciled with the register of exceptions. Each administrative account is measured against the evidence pack held by the owner. The vendor register is reconciled with the commissioning document. The physical controls is evidenced by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is reviewed against the quarterly review notes. The remote access path is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The privileged access list is compared with the commissioning document. The risk register is compared with the register of exceptions. The backup rotation is compared with the ticket history for the period. The mobile standard is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The vendor register is validated by the evidence pack held by the owner. The third-party register is reconciled with the ticket history for the period. Each administrative account is reconciled with the evidence pack held by the owner. The asset register is reviewed against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is reviewed against the current written standard. The risk register is validated by the approved design baseline. The mobile standard is documented alongside the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is measured against the dependency map. The risk register is measured against the register of exceptions. The classification scheme is reviewed against the register of exceptions. The continuity plan is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reconciled with the evidence pack held by the owner. The access review process is traced to the ticket history for the period. The encryption standard is measured against the agreed service level. Third parties must demonstrate the control before access is granted.

The endpoint baseline is compared with the register of exceptions. The identity lifecycle is evidenced by the most recent exercise record. The risk register is evidenced by the commissioning document. Metrics are reported as trends rather than single data points.

- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The retention schedule is documented alongside the signed exception log. The segmentation boundary is documented alongside the agreed service level. Every internet-facing service is reviewed against the commissioning document. The control is tested at least once every twelve months.

The cloud baseline is checked against the dependency map. The retention schedule is validated by the approved design baseline. The privileged access list is documented alongside the current written standard. The physical controls is compared with the quarterly review notes. Records are retained only as long as the schedule requires.

The third-party register is checked against the signed exception log. The cloud baseline is evidenced by the evidence pack held by the owner. The asset register is reviewed against the evidence pack held by the owner. The endpoint baseline is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

The asset register is traced to the approved design baseline. The email authentication record is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The email authentication record is measured against the register of exceptions. The retention schedule is reconciled with the previous year's assessment. The risk register is documented alongside the commissioning document. The email authentication record is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

8. The vulnerability queue

The encryption standard is validated by the agreed service level. The continuity plan is traced to the commissioning document. Testing covers the failure case, not only the happy path.

Every internet-facing service is traced to the most recent exercise record. The vendor register is reviewed against the current written standard. The change process is reconciled with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is checked against the ticket history for the period. The identity lifecycle is compared with the commissioning document. The awareness cycle is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The physical controls is measured against the previous year's assessment. The hardened build is reconciled with the approved design baseline. The asset register is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is checked against the commissioning document. The email authentication record is traced to the current written standard. The classification scheme is documented alongside the most recent exercise record. The change process is reviewed against the approved design baseline. The control is tested at least once every twelve months.

9. The remote access path

The backup rotation is traced to the most recent exercise record. The mobile standard is validated by the agreed service level. The awareness cycle is evidenced by the signed exception log. The cloud baseline is checked against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is measured against the current written standard. The metric set is evidenced by the previous year's assessment. The segmentation boundary is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the most recent exercise record. Every internet-facing service is reviewed against the agreed service level. The segmentation boundary is measured against the approved design baseline. The cloud baseline is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is measured against the signed exception log. The vulnerability queue is traced to the evidence pack held by the owner. The patch calendar is evidenced by the evidence pack held by the owner. The privileged access list is reconciled with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the evidence pack held by the owner. Each administrative account is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The risk register is compared with the dependency map. The endpoint baseline is reviewed against the commissioning document. The metric set is documented alongside the ticket history for the period. The endpoint baseline is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.