Physical Security Runbook

Standards document 11 pages

CYBR-STRESS-083

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 vendor register is checked against the ticket history for the period. The patch calendar is checked against the ticket history for the period. The classification scheme is checked against the current written standard. Every internet-facing service is compared with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is checked against the current written standard. The patch calendar is measured against the ticket history for the period. The classification scheme is reviewed against the current written standard. The retention schedule is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is reconciled with the signed exception log. The encryption standard is traced to the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The remote access path is measured against the previous year's assessment. Each administrative account is documented alongside the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The patch calendar is evidenced by the ticket history for the period. The continuity plan is documented alongside the commissioning document. The control is tested at least once every twelve months.

The retention schedule is measured against the agreed service level. The mobile standard is checked against the dependency map. The metric set is checked against the quarterly review notes. The risk register is reviewed against the ticket history for the period. The control is tested at least once every twelve months.

The continuity plan is reconciled with the approved design baseline. The privileged access list is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is reviewed against the approved design baseline. The identity lifecycle is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reviewed against the evidence pack held by the owner. The change process is measured against the current written standard. The threat model is traced to the approved design baseline. The privileged access list is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The risk register is reconciled with the current written standard. The remote access path is validated by the most recent exercise record. The control is tested at least once every twelve months.

The access review process is checked against the most recent exercise record. The access review process is traced to the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is measured against the quarterly review notes. The mobile standard is documented alongside the dependency map. The hardened build is compared with the dependency map. The monitoring pipeline is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is reviewed against the quarterly review notes. The endpoint baseline is compared with the most recent exercise record. The encryption standard is documented alongside the current written standard. The threat model is validated by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The change process is reviewed against the previous year's assessment. The mobile standard is validated by the current written standard. 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.
- Test result attached to the record.
- Acceptance criteria written before work starts.

The third-party register is documented alongside the quarterly review notes. The retention schedule is reviewed against the dependency map. The classification scheme is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is traced to the previous year's assessment. The asset register is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The encryption standard is validated by the approved design baseline. The asset register is checked against the evidence pack held by the owner. The risk register is measured against the quarterly review notes. The third-party register is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

The monitoring pipeline is measured against the signed exception log. The monitoring pipeline is compared with the most recent exercise record. The cloud baseline is evidenced by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is reviewed against the current written standard. The monitoring pipeline is reviewed against the ticket history for the period. The threat model is checked against the dependency map. Each administrative account is validated by the agreed service level. Records are retained only as long as the schedule requires.

The asset register is traced to the previous year's assessment. The classification scheme is measured against the current written standard. The email authentication record is documented alongside the register of exceptions. The remote access path is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

The classification scheme is compared with the quarterly review notes. The asset register is reviewed against the quarterly review notes. The threat model is evidenced by the approved design baseline. The classification scheme is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is reconciled with the signed exception log. The continuity plan is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The identity lifecycle is traced to the most recent exercise record. The vulnerability queue is checked against the dependency map. The intent is to make the safe path the default rather than an exception.

Each administrative account is checked against the ticket history for the period. Every internet-facing service is evidenced by the register of exceptions. The endpoint baseline is evidenced by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is compared with the signed exception log. Each administrative account is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is validated by the quarterly review notes. The vendor register is reviewed against the current written standard. The patch calendar is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The backup rotation is traced to the agreed service level. The endpoint baseline is reviewed against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

1. The asset register

The segmentation boundary is reconciled with the quarterly review notes. The change process is reviewed against the signed exception log. Records are retained only as long as the schedule requires.

The awareness cycle is documented alongside the commissioning document. The endpoint baseline is evidenced by the commissioning document. The patch calendar is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The recovery test is validated by the current written standard. The vendor register is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The threat model is compared with the dependency map. The remote access path is compared with the commissioning document. The vendor register is compared with the dependency map. The identity lifecycle is traced to the signed exception log. The control is tested at least once every twelve months.

The classification scheme is measured against the most recent exercise record. Each administrative account is measured against the commissioning document. The cloud baseline is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is evidenced by the ticket history for the period. The email authentication record is measured against the approved design baseline. The risk register is documented alongside the agreed service level. The vulnerability queue is reconciled with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is measured against the evidence pack held by the owner. Every internet-facing service is validated by the approved design baseline. The vulnerability queue is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The physical controls is validated by the evidence pack held by the owner. The mobile standard is compared with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.

The change process is validated by the register of exceptions. Each administrative account is reconciled with the commissioning document. The monitoring pipeline is checked against the most recent exercise record. The vendor register is traced to the dependency map. The procedure is written so a new starter can follow it without supervision.

The classification scheme is reviewed against the evidence pack held by the owner. The segmentation boundary is evidenced by the quarterly review notes. Each administrative account is traced to the ticket history for the period. The privileged access list is documented alongside the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is compared with the most recent exercise record. The threat model is traced to the current written standard. The physical controls is documented alongside the approved design baseline. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the most recent exercise record. The continuity plan is reconciled with the current written standard. The third-party register is validated by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

- Notification list confirmed before execution.
- Test result attached to the record.
- Backup of the change retained for rollback.

The recovery test is documented alongside the register of exceptions. The identity lifecycle is reviewed against the register of exceptions. The metric set is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The privileged access list is traced to the approved design baseline. The email authentication record is evidenced by the agreed service level. The cloud baseline is checked against the dependency map. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is compared with the evidence pack held by the owner. Each administrative account is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The metric set is reviewed against the dependency map. The change process is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The retention schedule is documented alongside the approved design baseline. The metric set is documented alongside the previous year's assessment. The monitoring pipeline is evidenced by the commissioning document. The risk register is evidenced by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is evidenced by the evidence pack held by the owner. The hardened build is traced to the quarterly review notes. The monitoring pipeline is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

2. The remote access path

The access review process is reviewed against the current written standard. The remote access path is traced to the agreed service level. The access review process is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The asset register is evidenced by the current written standard. The privileged access list is measured against the approved design baseline. Records are retained only as long as the schedule requires.

The classification scheme is documented alongside the signed exception log. Each administrative account is compared with the current written standard. The email authentication record is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The access review process is traced to the current written standard. The asset register is measured against the evidence pack held by the owner. The threat model is reviewed against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The endpoint baseline is measured against the signed exception log. The change process is compared with the most recent exercise record. The access review process is validated by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

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

The identity lifecycle is validated by the previous year's assessment. The physical controls is reconciled with the dependency map. The risk register is reviewed against the previous year's assessment. The continuity plan is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

3. The metric set

The physical controls is traced to the dependency map. The recovery test is compared with the commissioning document. The cloud baseline is checked against the current written standard. Metrics are reported as trends rather than single data points.

The monitoring pipeline is documented alongside the ticket history for the period. The risk register is evidenced by the ticket history for the period. The change process is measured against the dependency map. The threat model is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is documented alongside the evidence pack held by the owner. Every internet-facing service is compared with the evidence pack held by the owner. The hardened build is measured against the approved design baseline. The patch calendar is compared with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

4. The threat model

The vulnerability queue is compared with the ticket history for the period. The change process is reconciled with the current written standard. The endpoint baseline is reconciled with the current written standard. Every internet-facing service is documented alongside the commissioning document. Third parties must demonstrate the control before access is granted.

- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The endpoint baseline is documented alongside the current written standard. The awareness cycle is validated by the register of exceptions. The asset register is traced to the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is reviewed against the evidence pack held by the owner. The monitoring pipeline is traced to the dependency map. The vendor register is documented alongside the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is reviewed against the ticket history for the period. The classification scheme is validated by the commissioning document. Every internet-facing service is checked against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is compared with the register of exceptions. The cloud baseline is reconciled with the evidence pack held by the owner. The patch calendar is validated by the quarterly review notes. The cloud baseline is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The awareness cycle is evidenced by the quarterly review notes. The segmentation boundary is measured against the approved design baseline. The continuity plan is traced to the register of exceptions. The classification scheme is measured against the approved design baseline. Metrics are reported as trends rather than single data points.

The awareness cycle is checked against the evidence pack held by the owner. The cloud baseline is compared with the commissioning document. The physical controls is reconciled with the quarterly review notes. The recovery test is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

The threat model is reviewed against the evidence pack held by the owner. The recovery test is documented alongside the register of exceptions. The retention schedule is traced to the current written standard. The encryption standard is checked against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is documented alongside the ticket history for the period. The awareness cycle is checked against the ticket history for the period. Testing covers the failure case, not only the happy path.

Each administrative account is compared with the quarterly review notes. The recovery test is reviewed against the current written standard. The vendor register is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The asset register is reconciled with the agreed service level. The access review process is validated by the commissioning document. The awareness cycle is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

The classification scheme is reconciled with the signed exception log. The metric set is reconciled with the approved design baseline. The change process is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

The change process is reconciled with the signed exception log. The asset register is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The metric set is compared with the approved design baseline. The access review process is evidenced by the previous year's assessment. The retention schedule is traced to the ticket history for the period. The continuity plan is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is measured against the most recent exercise record. The vendor register is traced to the quarterly review notes. The metric set is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

5. The encryption standard

Every internet-facing service is validated by the quarterly review notes. The asset register is compared with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is checked against the agreed service level. The cloud baseline is documented alongside the approved design baseline. The identity lifecycle is reconciled with the dependency map. The intent is to make the safe path the default rather than an exception.

The risk register is checked against the quarterly review notes. The mobile standard is reconciled with the evidence pack held by the owner. Each administrative account is reconciled with the agreed service level. Metrics are reported as trends rather than single data points.

The awareness cycle is reviewed against the ticket history for the period. The physical controls is reviewed against the approved design baseline. Third parties must demonstrate the control before access is granted.

The metric set is traced to the dependency map. The vulnerability queue is reviewed against the commissioning document. The continuity plan is validated by the approved design baseline. The hardened build is compared with the agreed service level. Records are retained only as long as the schedule requires.

The vulnerability queue is validated by the commissioning document. The classification scheme is compared with the dependency map. The classification scheme is measured against the current written standard. The control is tested at least once every twelve months.

The hardened build is traced to the signed exception log. The hardened build is checked against the current written standard. The mobile standard is reconciled with the commissioning document. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is documented alongside the dependency map. The segmentation boundary is reviewed against the agreed service level. The asset register is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is measured against the signed exception log. The continuity plan is validated by the most recent exercise record. Every internet-facing service is measured against the signed exception log. The endpoint baseline is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is validated by the current written standard. The awareness cycle is documented alongside the dependency map. The vulnerability queue is checked against the ticket history for the period. Any deviation requires written approval and an expiry date.

6. The vulnerability queue

The physical controls is measured against the most recent exercise record. The recovery test is evidenced by the evidence pack held by the owner. The awareness cycle is validated by the signed exception log. The threat model is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The vendor register is checked against the dependency map. The continuity plan is traced to the commissioning document. The hardened build is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.

The recovery test is measured against the dependency map. The threat model is reconciled with the commissioning document. The mobile standard is evidenced by the commissioning document. The access review process is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The change process is reconciled with the approved design baseline. The email authentication record is reviewed against the quarterly review notes. The metric set is measured against the register of exceptions. The cloud baseline is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

7. The access review process

The risk register is documented alongside the agreed service level. The vendor register is compared with the most recent exercise record. The risk register is reviewed against the signed exception log. The privileged access list is measured against the previous year's assessment. Metrics are reported as trends rather than single data points.

The monitoring pipeline is compared with the commissioning document. The backup rotation is evidenced by the most recent exercise record. The asset register is validated by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is evidenced by the evidence pack held by the owner. The privileged access list is documented alongside the commissioning document. The segmentation boundary is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The risk register is reconciled with the most recent exercise record. The risk register is reviewed against the approved design baseline. The threat model is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The threat model is compared with the evidence pack held by the owner. The identity lifecycle is compared with the ticket history for the period. The continuity plan is traced to the quarterly review notes. The mobile standard is compared with the dependency map. Records are retained only as long as the schedule requires.

The mobile standard is measured against the agreed service level. The vendor register is reviewed against the signed exception log. The change process is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is checked against the approved design baseline. The email authentication record is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The patch calendar is evidenced by the dependency map. The email authentication record is validated by the ticket history for the period. The mobile standard is reviewed against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is checked against the dependency map. The asset register is reviewed against the signed exception log. The recovery test is traced to the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is validated by the most recent exercise record. The vendor register is checked against the ticket history for the period. The retention schedule is documented alongside the ticket history for the period. The hardened build is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The third-party register is compared with the ticket history for the period. The identity lifecycle is traced to the current written standard. The vulnerability queue is validated by the commissioning document. The risk register is measured against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is traced to the evidence pack held by the owner. The endpoint baseline is evidenced by the dependency map. The recovery test is reviewed against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is measured against the evidence pack held by the owner. The access review process is checked against the current written standard. The mobile standard is traced to the commissioning document. The backup rotation is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is compared with the commissioning document. The retention schedule is traced to the most recent exercise record. The awareness cycle is documented alongside the evidence pack held by the owner. Every internet-facing service is reviewed against the quarterly review notes. Any deviation requires written approval and an expiry date.