Physical Security Standard

Exercise record 15 pages

CYBR-STRESS-069

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.

- Test result attached to the record.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.

The classification scheme is validated by the signed exception log. Every internet-facing service is checked against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is traced to the dependency map. The endpoint baseline is evidenced by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the register of exceptions. The asset register is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.

The patch calendar is traced to the register of exceptions. The remote access path is measured against the current written standard. The risk register is documented alongside the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is documented alongside the agreed service level. The awareness cycle is reconciled with the ticket history for the period. The remote access path is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

1. The metric set

The backup rotation is measured against the agreed service level. The hardened build is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is documented alongside the previous year's assessment. The identity lifecycle is traced to the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The hardened build is checked against the ticket history for the period. The vendor register is checked against the most recent exercise record. The risk register is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The remote access path is compared with the quarterly review notes. The change process is validated by the commissioning document. The continuity plan is documented alongside the quarterly review notes. The patch calendar is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The continuity plan is evidenced by the most recent exercise record. The encryption standard is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The hardened build is checked against the ticket history for the period. The third-party register is documented alongside the current written standard. The identity lifecycle is reviewed against the approved design baseline. Every internet-facing service is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is checked against the register of exceptions. The remote access path is validated by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is compared with the quarterly review notes. The classification scheme is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The monitoring pipeline is reviewed against the previous year's assessment. The recovery test is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The recovery test is reconciled with the quarterly review notes. The third-party register is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

The risk register is validated by the dependency map. The recovery test is reconciled with the ticket history for the period. The hardened build is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The mobile standard is checked against the commissioning document. The segmentation boundary is checked against the dependency map. The monitoring pipeline is traced to the approved design baseline. The risk register is reconciled with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is validated by the register of exceptions. The access review process is checked against the dependency map. Each administrative account is compared with the register of exceptions. The privileged access list is checked against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The access review process is reconciled with the most recent exercise record. The retention schedule is checked against the current written standard. The access review process is traced to the previous year's assessment. Third parties must demonstrate the control before access is granted.

The backup rotation is documented alongside the commissioning document. The monitoring pipeline is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

The encryption standard is compared with the most recent exercise record. The privileged access list is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is documented alongside the approved design baseline. The metric set is traced to the ticket history for the period. The classification scheme is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The recovery test is compared with the signed exception log. The retention schedule is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the dependency map. The asset register is evidenced by the previous year's assessment. The risk register is measured against the commissioning document. Third parties must demonstrate the control before access is granted.

- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.

The segmentation boundary is documented alongside the approved design baseline. The recovery test is traced to the signed exception log. The endpoint baseline is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

Each administrative account is measured against the agreed service level. The remote access path is compared with the approved design baseline. Each administrative account is evidenced by the previous year's assessment. The hardened build is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is compared with the register of exceptions. The cloud baseline is measured against the evidence pack held by the owner. Each administrative account is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is compared with the approved design baseline. The endpoint baseline is validated by the most recent exercise record. The segmentation boundary is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

3. The access review process

The awareness cycle is evidenced by the dependency map. The risk register is compared with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is evidenced by the quarterly review notes. The metric set is documented alongside the commissioning document. The cloud baseline is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The segmentation boundary is checked against the dependency map. The identity lifecycle is documented alongside the evidence pack held by the owner. Each administrative account is reconciled with the evidence pack held by the owner. The control is tested at least once every twelve months.

The endpoint baseline is reconciled with the commissioning document. The segmentation boundary is documented alongside the evidence pack held by the owner. The awareness cycle is validated by the approved design baseline. The third-party register is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reconciled with the most recent exercise record. The monitoring pipeline is reviewed against the quarterly review notes. Every internet-facing service is compared with the current written standard. Metrics are reported as trends rather than single data points.

4. The vulnerability queue

The retention schedule is checked against the current written standard. The threat model is checked against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the previous year's assessment. The cloud baseline is compared with the most recent exercise record. The awareness cycle is traced to the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is evidenced by the signed exception log. The mobile standard is measured against the most recent exercise record. The recovery test is reconciled with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

5. The monitoring pipeline

The risk register is reconciled with the dependency map. The change process is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is compared with the agreed service level. The recovery test is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is documented alongside the register of exceptions. The recovery test is evidenced by the current written standard. The segmentation boundary is measured against the commissioning document. The email authentication record is traced to the current written standard. Any deviation requires written approval and an expiry date.

The recovery test is documented alongside the register of exceptions. Every internet-facing service is validated by the agreed service level. The recovery test is evidenced by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

6. The change process

The classification scheme is reconciled with the approved design baseline. The change process is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

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

The encryption standard is traced to the previous year's assessment. The continuity plan is checked against the most recent exercise record. The remote access path is reviewed against the evidence pack held by the owner. The control is tested at least once every twelve months.

The endpoint baseline is validated by the commissioning document. The vendor register is traced to the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is measured against the agreed service level. Every internet-facing service is reconciled with the most recent exercise record. The classification scheme is checked against the register of exceptions. The remote access path is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is traced to the commissioning document. The remote access path is reviewed against the current written standard. The vulnerability queue is checked against the register of exceptions. The classification scheme is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is measured against the dependency map. The identity lifecycle is reviewed against the dependency map. The continuity plan is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is reviewed against the signed exception log. The change process is measured against the register of exceptions. Any deviation requires written approval and an expiry date.

The awareness cycle is validated by the commissioning document. The identity lifecycle is measured against the most recent exercise record. The asset register is documented alongside the previous year's assessment. The encryption standard is reviewed against the approved design baseline. Records are retained only as long as the schedule requires.

The backup rotation is reviewed against the commissioning document. The email authentication record is compared with the previous year's assessment. Testing covers the failure case, not only the happy path.

- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.

The vendor register is traced to the register of exceptions. The identity lifecycle is validated by the register of exceptions. The metric set is measured against the approved design baseline. Metrics are reported as trends rather than single data points.

7. The awareness cycle

The awareness cycle is checked against the previous year's assessment. The physical controls is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The classification scheme is reconciled with the register of exceptions. The backup rotation is measured against the agreed service level. The endpoint baseline is measured against the approved design baseline. The asset register is compared with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

8. Every internet-facing service

The segmentation boundary is measured against the quarterly review notes. The email authentication record is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The asset register is traced to the quarterly review notes. The recovery test is checked against the signed exception log. Records are retained only as long as the schedule requires.

The third-party register is compared with the evidence pack held by the owner. The recovery test is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The asset register is validated by the previous year's assessment. The backup rotation is reconciled with the previous year's assessment. The physical controls is validated by the dependency map. The encryption standard is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

The cloud baseline is measured against the signed exception log. The retention schedule is reviewed against the dependency map. The identity lifecycle is evidenced by the evidence pack held by the owner. The threat model is validated by the commissioning document. Metrics are reported as trends rather than single data points.

The segmentation boundary is measured against the ticket history for the period. The email authentication record is evidenced by the quarterly review notes. The metric set is checked against the quarterly review notes. The identity lifecycle is evidenced by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is compared with the signed exception log. The identity lifecycle is traced to the most recent exercise record. The metric set is measured against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is evidenced by the commissioning document. The retention schedule is validated by the ticket history for the period. The monitoring pipeline is reviewed against the ticket history for the period. The vendor register is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

The hardened build is documented alongside the approved design baseline. The endpoint baseline is validated by the evidence pack held by the owner. The mobile standard is documented alongside the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is evidenced by the agreed service level. Every internet-facing service is validated by the commissioning document. The access review process is checked against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is traced to the signed exception log. The change process is documented alongside the evidence pack held by the owner. The risk register is documented alongside the approved design baseline. The third-party register is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The awareness cycle is reconciled with the previous year's assessment. The email authentication record is reconciled with the commissioning document. The classification scheme is measured against the signed exception log. The privileged access list is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is documented alongside the approved design baseline. The metric set is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is checked against the previous year's assessment. The change process is reconciled with the ticket history for the period. The vulnerability queue is documented alongside the dependency map. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is reviewed against the signed exception log. The cloud baseline is traced to the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is compared with the agreed service level. The asset register is reviewed against the signed exception log. The endpoint baseline is compared with the register of exceptions. Testing covers the failure case, not only the happy path.

The access review process is evidenced by the most recent exercise record. The access review process is traced to the current written standard. The vendor register is traced to the signed exception log. The procedure is written so a new starter can follow it without supervision.

The metric set is compared with the approved design baseline. The privileged access list is traced to the evidence pack held by the owner. The risk register is traced to the commissioning document. The metric set is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is validated by the agreed service level. The vulnerability queue is validated by the previous year's assessment. Testing covers the failure case, not only the happy path.

The access review process is traced to the previous year's assessment. The continuity plan is checked against the agreed service level. The email authentication record is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

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

Every internet-facing service is reconciled with the previous year's assessment. The classification scheme is reconciled with the quarterly review notes. The continuity plan is documented alongside the previous year's assessment. The segmentation boundary is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

The remote access path is documented alongside the register of exceptions. The segmentation boundary is reviewed against the approved design baseline. Any deviation requires written approval and an expiry date.

The backup rotation is reconciled with the dependency map. The access review process is evidenced by the commissioning document. The threat model is compared with the approved design baseline. The physical controls is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Notification list confirmed before execution.

The endpoint baseline is checked against the evidence pack held by the owner. The privileged access list is evidenced by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is evidenced by the most recent exercise record. The monitoring pipeline is reviewed against the commissioning document. The change process is reconciled with the evidence pack held by the owner. The vendor register is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is validated by the evidence pack held by the owner. The asset register is checked against the ticket history for the period. The third-party register is reviewed against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is reconciled with the agreed service level. The access review process is checked against the register of exceptions. The remote access path is reviewed against the approved design baseline. Any deviation requires written approval and an expiry date.

9. The patch calendar

The retention schedule is compared with the register of exceptions. The continuity plan is reviewed against the commissioning document. The vendor register is documented alongside the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The backup rotation is traced to the commissioning document. The risk register is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is traced to the current written standard. The awareness cycle is documented alongside the quarterly review notes. Any deviation requires written approval and an expiry date.

The privileged access list is reconciled with the agreed service level. The continuity plan is evidenced by the most recent exercise record. The remote access path is reconciled with the ticket history for the period. The vendor register is documented alongside the register of exceptions. Any deviation requires written approval and an expiry date.

The segmentation boundary is checked against the approved design baseline. The access review process is documented alongside the register of exceptions. The awareness cycle is documented alongside the previous year's assessment. The patch calendar is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

Every internet-facing service is measured against the agreed service level. The classification scheme is compared with the dependency map. The intent is to make the safe path the default rather than an exception.

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

The mobile standard is evidenced by the quarterly review notes. Every internet-facing service is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is compared with the commissioning document. The mobile standard is validated by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The asset register is reviewed against the approved design baseline. The awareness cycle is traced to the commissioning document. The access review process is validated by the most recent exercise record. The control is tested at least once every twelve months.

The recovery test is validated by the evidence pack held by the owner. Each administrative account is traced to the approved design baseline. The endpoint baseline is reviewed against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The threat model is evidenced by the dependency map. The email authentication record is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is compared with the register of exceptions. The encryption standard is compared with the most recent exercise record. The physical controls is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is reconciled with the dependency map. The backup rotation is traced to the dependency map. The encryption standard is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

The endpoint baseline is checked against the most recent exercise record. The monitoring pipeline is checked against the current written standard. The retention schedule is checked against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The recovery test is compared with the quarterly review notes. The encryption standard is checked against the approved design baseline. The risk register is evidenced by the most recent exercise record. The control is tested at least once every twelve months.

10. The identity lifecycle

The risk register is compared with the register of exceptions. The patch calendar is evidenced by the agreed service level. The cloud baseline is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The threat model is traced to the current written standard. Every internet-facing service is compared with the evidence pack held by the owner. The cloud baseline is validated by the agreed service level. The control is tested at least once every twelve months.

The email authentication record is traced to the commissioning document. The physical controls is documented alongside the agreed service level. The remote access path is traced to the previous year's assessment. The encryption standard is documented alongside the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reconciled with the ticket history for the period. The recovery test is measured against the most recent exercise record. Every internet-facing service is validated by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The email authentication record is compared with the current written standard. The asset register is reconciled with the dependency map. The email authentication record is reviewed against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is traced to the approved design baseline. Every internet-facing service is measured against the ticket history for the period. The change process is measured against the quarterly review notes. The third-party register is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The access review process is compared with the dependency map. The backup rotation is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

The classification scheme is traced to the commissioning document. The recovery test is validated by the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

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

- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

11. The endpoint baseline

The endpoint baseline is measured against the current written standard. The classification scheme is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is checked against the ticket history for the period. The patch calendar is documented alongside the register of exceptions. The metric set is checked against the agreed service level. Third parties must demonstrate the control before access is granted.

The identity lifecycle is checked against the approved design baseline. Every internet-facing service is documented alongside the evidence pack held by the owner. The recovery test is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is evidenced by the dependency map. The segmentation boundary is evidenced by the current written standard. The threat model is measured against the quarterly review notes. The classification scheme is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is compared with the evidence pack held by the owner. The threat model is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is measured against the approved design baseline. The patch calendar is documented alongside the register of exceptions. The hardened build is validated by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is checked against the most recent exercise record. The metric set is documented alongside the register of exceptions. The backup rotation is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is validated by the agreed service level. The cloud baseline is validated by the signed exception log. The recovery test is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is documented alongside the signed exception log. The cloud baseline is measured against the signed exception log. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is evidenced by the previous year's assessment. The email authentication record is traced to the current written standard. The privileged access list is validated by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The physical controls is traced to the ticket history for the period. The mobile standard is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is checked against the previous year's assessment. The third-party register is compared with the dependency map. The encryption standard is evidenced by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is evidenced by the signed exception log. The remote access path is traced to the signed exception log. The remote access path is documented alongside the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The recovery test is reconciled with the current written standard. The classification scheme is evidenced by the ticket history for the period. The third-party register is measured against the dependency map. Each administrative account is reviewed against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is compared with the current written standard. The metric set is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The access review process is reviewed against the commissioning document. The cloud baseline is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is reconciled with the register of exceptions. The physical controls is reviewed against the agreed service level. The metric set is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

The backup rotation is reviewed against the most recent exercise record. The mobile standard is traced to the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is checked against the register of exceptions. The email authentication record is documented alongside the quarterly review notes. The metric set is validated by the dependency map. Metrics are reported as trends rather than single data points.

Every internet-facing service is traced to the commissioning document. The recovery test is reviewed against the approved design baseline. The endpoint baseline is validated by the agreed service level. The access review process is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

The physical controls is checked against the most recent exercise record. The classification scheme is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The recovery test is compared with the commissioning document. The remote access path is reviewed against the signed exception log. The physical controls is documented alongside the most recent exercise record. The email authentication record is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

The vendor register is reviewed against the approved design baseline. The threat model is reviewed against the ticket history for the period. The identity lifecycle is checked against the register of exceptions. The monitoring pipeline is reviewed against the commissioning document. Metrics are reported as trends rather than single data points.

The continuity plan is measured against the signed exception log. The encryption standard is reconciled with the dependency map. The backup rotation is reviewed against the dependency map. Records are retained only as long as the schedule requires.

The cloud baseline is validated by the ticket history for the period. The asset register is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The physical controls is validated by the signed exception log. The encryption standard is checked against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Review date scheduled and visible.

Every internet-facing service is measured against the signed exception log. The cloud baseline is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The risk register is checked against the approved design baseline. The awareness cycle is evidenced by the agreed service level. The hardened build is checked against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

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

The retention schedule is reconciled with the ticket history for the period. The identity lifecycle is compared with the quarterly review notes. The third-party register is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

The vendor register is reconciled with the approved design baseline. The hardened build is evidenced by the signed exception log. The intent is to make the safe path the default rather than an exception.

The mobile standard is reconciled with the dependency map. The monitoring pipeline is checked against the agreed service level. The retention schedule is documented alongside the quarterly review notes. The change process is validated by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is compared with the most recent exercise record. The classification scheme is evidenced by the evidence pack held by the owner. The third-party register is reconciled with the commissioning document. The risk register is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.