Security Metrics Review

Exercise record 19 pages

CYBR-STRESS-099

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.

Each administrative account is reconciled with the evidence pack held by the owner. The mobile standard is checked against the quarterly review notes. The classification scheme is compared with the most recent exercise record. Testing covers the failure case, not only the happy path.

The classification scheme is reconciled with the signed exception log. The classification scheme is compared with the dependency map. The mobile standard is measured against the ticket history for the period. The control is tested at least once every twelve months.

The change process is traced to the previous year's assessment. The third-party register is traced to the signed exception log. The retention schedule is reconciled with the ticket history for the period. The remote access path is reviewed against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is validated by the agreed service level. The classification scheme is reconciled with the evidence pack held by the owner. The remote access path is compared with the agreed service level. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.

The recovery test is validated by the agreed service level. Every internet-facing service is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The email authentication record is validated by the signed exception log. Every internet-facing service is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The encryption standard is reconciled with the dependency map. The privileged access list is compared with the ticket history for the period. The asset register is reviewed against the evidence pack held by the owner. The identity lifecycle is compared with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The threat model is evidenced by the ticket history for the period. The third-party register is compared with the agreed service level. The mobile standard is measured 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 metric set is measured against the previous year's assessment. The remote access path is measured against the previous year's assessment. The identity lifecycle is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reconciled with the ticket history for the period. The remote access path is reviewed against the dependency map. Metrics are reported as trends rather than single data points.

The backup rotation is evidenced by the approved design baseline. The email authentication record is measured against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The vendor register is compared with the register of exceptions. The cloud baseline is checked against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Test result attached to the record.
- Notification list confirmed before execution.

The retention schedule is reviewed against the current written standard. The patch calendar is checked against the register of exceptions. Third parties must demonstrate the control before access is granted.

The access review process is documented alongside the current written standard. The monitoring pipeline is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The change process is documented alongside the quarterly review notes. The recovery test is traced to the register of exceptions. Third parties must demonstrate the control before access is granted.

The retention schedule is validated by the quarterly review notes. Each administrative account is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

1. Each administrative account

The cloud baseline is evidenced by the approved design baseline. The access review process is evidenced by the signed exception log. The classification scheme is compared with the ticket history for the period. The segmentation boundary is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The metric set is checked against the register of exceptions. The endpoint baseline is measured against the most recent exercise record. The mobile standard is measured against the evidence pack held by the owner. The email authentication record is validated by 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 identity lifecycle is reviewed against the dependency map. Every internet-facing service is traced to the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is checked against the register of exceptions. The email authentication record is reconciled with the register of exceptions. Every internet-facing service is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is reconciled with the agreed service level. The vendor register is checked against the commissioning document. The retention schedule is traced to the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is reconciled with the most recent exercise record. The third-party register is validated by the current written standard. Evidence is kept for audit, insurance and regulator requests.

- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The recovery test is reconciled with the dependency map. The backup rotation is checked against the current written standard. Records are retained only as long as the schedule requires.

The patch calendar is measured against the most recent exercise record. The asset register is measured against the previous year's assessment. Any deviation requires written approval and an expiry date.

The retention schedule is compared with the previous year's assessment. The physical controls is measured against the commissioning document. The change process is reconciled with the current written standard. The remote access path is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is evidenced by the approved design baseline. The cloud baseline is traced to the evidence pack held by the owner. The monitoring pipeline is measured against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is checked against the register of exceptions. The threat model is reviewed against the dependency map. The physical controls is reconciled with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

2. The vendor register

The endpoint baseline is compared with the agreed service level. The vendor register is compared with the signed exception log. The hardened build is measured against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is reviewed against the approved design baseline. The asset register is compared with the commissioning document. The privileged access list is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is reconciled with the previous year's assessment. The access review process is compared with the most recent exercise record. Testing covers the failure case, not only the happy path.

The endpoint baseline is measured against the signed exception log. The privileged access list is compared with the previous year's assessment. The asset register is evidenced by the commissioning document. The privileged access list is validated by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The hardened build is reconciled with the previous year's assessment. The remote access path is documented alongside the previous year's assessment. The awareness cycle is compared with the quarterly review notes. The retention schedule is compared with the current written standard. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is traced to the agreed service level. The risk register is traced to the current written standard. Records are retained only as long as the schedule requires.

- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The asset register is traced to the dependency map. The segmentation boundary is evidenced by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is validated by the commissioning document. The patch calendar is documented alongside the register of exceptions. The physical controls is measured against the agreed service level. Third parties must demonstrate the control before access is granted.

Every internet-facing service is checked against the previous year's assessment. The classification scheme is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is validated by the commissioning document. The third-party register is evidenced by the current written standard. The hardened build is traced to the most recent exercise record. Each administrative account is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is documented alongside the quarterly review notes. The hardened build is validated by the dependency map. The email authentication record is checked against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The remote access path is reviewed against the quarterly review notes. The recovery test is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is reconciled with the ticket history for the period. The continuity plan is checked against the approved design baseline. The monitoring pipeline is validated by the dependency map. The vendor register is documented alongside the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is checked against the quarterly review notes. The third-party register is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The asset register is reconciled with the commissioning document. The patch calendar is traced to the previous year's assessment. The threat model is validated by the register of exceptions. The hardened build is documented alongside the signed exception log. Metrics are reported as trends rather than single data points.

The risk register is evidenced by the current written standard. The vendor register is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The backup rotation is checked against the dependency map. The monitoring pipeline is evidenced by the evidence pack held by the owner. The patch calendar is traced to the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is traced to the most recent exercise record. The segmentation boundary is measured against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is reconciled with the quarterly review notes. The retention schedule is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The endpoint baseline is traced to the evidence pack held by the owner. The third-party register is traced to the commissioning document. The retention schedule is validated by the current written standard. The vendor register is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is checked against the most recent exercise record. The awareness cycle is measured against the approved design baseline. The monitoring pipeline is evidenced by the agreed service level. The third-party register is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The access review process is reconciled with the most recent exercise record. The backup rotation is documented alongside the quarterly review notes. The continuity plan is checked against the commissioning document. The asset register is traced to the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is compared with the evidence pack held by the owner. The encryption standard is reviewed against the approved design baseline. Every internet-facing service is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is validated by the commissioning document. The metric set is evidenced by the previous year's assessment. The recovery test is evidenced by the register of exceptions. The continuity plan is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The asset register is measured against the commissioning document. The retention schedule is reviewed against the evidence pack held by the owner. The awareness cycle is reconciled with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The third-party register is compared with the most recent exercise record. The backup rotation is checked against the commissioning document. The identity lifecycle is compared with the signed exception log. The privileged access list is compared with the signed exception log. The control is tested at least once every twelve months.

The email authentication record is traced to the evidence pack held by the owner. The change process is checked against the previous year's assessment. The classification scheme is measured against the previous year's assessment. The risk register is validated by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The metric set is evidenced by the approved design baseline. The vendor register is evidenced by the approved design baseline. The change process is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is traced to the previous year's assessment. The metric set is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The vulnerability queue is traced to the previous year's assessment. The patch calendar is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is measured against the ticket history for the period. The identity lifecycle is reviewed against the approved design baseline. The metric set is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The cloud baseline is reviewed against the evidence pack held by the owner. The email authentication record is documented alongside the previous year's assessment. The metric set is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is traced to the previous year's assessment. The awareness cycle is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The risk register is reconciled with the evidence pack held by the owner. The risk register is documented alongside the ticket history for the period. The hardened build is compared with the register of exceptions. Metrics are reported as trends rather than single data points.

The identity lifecycle is reviewed against the current written standard. The segmentation boundary is evidenced by the agreed service level. The hardened build is traced to the current written standard. The third-party register is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is documented alongside the quarterly review notes. Each administrative account is reviewed against the dependency map. Each administrative account is documented alongside the current written standard. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is measured against the dependency map. The asset register is traced to the signed exception log. The vulnerability queue is reconciled with the approved design baseline. The identity lifecycle is validated by the quarterly review notes. Testing covers the failure case, not only the happy path.

The access review process is measured against the register of exceptions. The physical controls is traced to the register of exceptions. The access review process is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

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

The continuity plan is reviewed against the dependency map. The retention schedule is checked against the dependency map. The encryption standard is compared with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is reconciled with the ticket history for the period. The email authentication record is reviewed against the register of exceptions. The continuity plan is measured against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The access review process is evidenced by the dependency map. The asset register is documented alongside the current written standard. The cloud baseline is reviewed against the evidence pack held by the owner. The control is tested at least once every twelve months.

The email authentication record is documented alongside the dependency map. The access review process is reviewed against the signed exception log. The access review process is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The cloud baseline is documented alongside the commissioning document. The vendor register is validated by the current written standard. The control is tested at least once every twelve months.

The physical controls is documented alongside the previous year's assessment. The identity lifecycle is measured against the signed exception log. The email authentication record is measured against the commissioning document. Third parties must demonstrate the control before access is granted.

The cloud baseline is measured against the dependency map. Every internet-facing service is compared with the approved design baseline. The encryption standard is evidenced by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is traced to the register of exceptions. The awareness cycle is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.

Each administrative account is measured against the quarterly review notes. The identity lifecycle is compared with the quarterly review notes. The physical controls is documented alongside the register of exceptions. Every internet-facing service is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

The remote access path is reviewed against the agreed service level. The access review process is evidenced by the most recent exercise record. The cloud baseline is evidenced by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reconciled with the signed exception log. The backup rotation is evidenced by the register of exceptions. The endpoint baseline is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The risk register is reviewed against the most recent exercise record. The backup rotation is validated by the current written standard. Any deviation requires written approval and an expiry date.

The identity lifecycle is reconciled with the most recent exercise record. The email authentication record is measured against the agreed service level. The hardened build is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The hardened build is documented alongside the ticket history for the period. The classification scheme is checked against the signed exception log. The asset register is reviewed against the current written standard. Every internet-facing service is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is evidenced by the dependency map. The third-party register is checked against the approved design baseline. The backup rotation is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The risk register is documented alongside the ticket history for the period. The email authentication record is reviewed against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is reviewed against the commissioning document. The continuity plan is checked against the current written standard. The identity lifecycle is compared with the dependency map. The awareness cycle is traced to the dependency map. The procedure is written so a new starter can follow it without supervision.

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

The encryption standard is reconciled with the register of exceptions. The access review process is checked against the agreed service level. The segmentation boundary is evidenced by the current written standard. The monitoring pipeline is measured against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is measured against the signed exception log. The endpoint baseline is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The threat model is evidenced by the register of exceptions. The awareness cycle is checked against the current written standard. The encryption standard is reconciled with the signed exception log. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the signed exception log. The asset register is checked against the evidence pack held by the owner. The physical controls is compared with the most recent exercise record. The endpoint baseline is validated by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is validated by the dependency map. Each administrative account is reconciled with the most recent exercise record. The risk register is traced to the ticket history for the period. The recovery test is evidenced by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is compared with the dependency map. The backup rotation is reviewed against the previous year's assessment. The retention schedule is validated by the dependency map. The asset register is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The change process is documented alongside the ticket history for the period. The privileged access list is compared with the register of exceptions. The cloud baseline is reviewed against the current written standard. The threat model 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 remote access path is documented alongside the current written standard. The metric set is reviewed against the ticket history for the period. The awareness cycle is evidenced by the most recent exercise record. The classification scheme is compared with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The remote access path is validated by the agreed service level. The patch calendar is checked against the agreed service level. The risk register is validated by the evidence pack held by the owner. The remote access path is evidenced by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The mobile standard is reviewed against the previous year's assessment. The risk register is reviewed against the quarterly review notes. The recovery test is validated by the previous year's assessment. The metric set is reconciled with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is traced to the commissioning document. The backup rotation is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

The encryption standard is validated by the most recent exercise record. The awareness cycle is evidenced by the previous year's assessment. The metric set is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The vendor register is reviewed against the current written standard. The asset register is compared with the commissioning document. The third-party register is measured against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is checked against the register of exceptions. The hardened build is validated by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The metric set is reviewed against the dependency map. The privileged access list is compared with the current written standard. The asset register is reconciled with the dependency map. The retention schedule is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is checked against the ticket history for the period. The threat model is reconciled with the agreed service level. The third-party register is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is measured against the register of exceptions. The change process is traced to the dependency map. The risk register is traced to the approved design baseline. Each administrative account is checked against the signed exception log. Metrics are reported as trends rather than single data points.

The awareness cycle is measured against the quarterly review notes. The patch calendar is compared with the evidence pack held by the owner. The access review process is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is traced to the current written standard. The change process is compared with the current written standard. The threat model is measured against the current written standard. The asset register is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is evidenced by the current written standard. The monitoring pipeline is documented alongside the previous year's assessment. The backup rotation is reviewed against the evidence pack held by the owner. The vendor register is documented alongside the quarterly review notes. Metrics are reported as trends rather than single data points.

Each administrative account is traced to the previous year's assessment. The segmentation boundary is documented alongside the dependency map. The threat model is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is reconciled with the ticket history for the period. The backup rotation is reconciled with the dependency map. Every internet-facing service is documented alongside the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The backup rotation is documented alongside the register of exceptions. The continuity plan is evidenced by the approved design baseline. The mobile standard is evidenced by the register of exceptions. The retention schedule is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is evidenced by the agreed service level. The hardened build is documented alongside the quarterly review notes. The cloud baseline is reviewed against the register of exceptions. The hardened build is compared with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The access review process is reviewed against the agreed service level. The segmentation boundary is validated by the commissioning document. The access review process is reconciled with the previous year's assessment. Testing covers the failure case, not only the happy path.

The risk register is validated by the commissioning document. The change process is reconciled with the dependency map. The segmentation boundary is documented alongside the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is compared with the previous year's assessment. The cloud baseline is reviewed against the ticket history for the period. Every internet-facing service is traced to the commissioning document. Any deviation requires written approval and an expiry date.

The awareness cycle is evidenced by the most recent exercise record. The awareness cycle is traced to the evidence pack held by the owner. The segmentation boundary is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The email authentication record is reviewed against the current written standard. The identity lifecycle is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The cloud baseline is validated by the quarterly review notes. The metric set is traced to the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is measured against the signed exception log. The asset register is documented alongside the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is validated by the previous year's assessment. The change process is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is evidenced by the approved design baseline. The mobile standard is documented alongside the dependency map. The endpoint baseline is reconciled with 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.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.

The metric set is evidenced by the previous year's assessment. The endpoint baseline is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

Each administrative account is documented alongside the register of exceptions. Every internet-facing service is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

The identity lifecycle is evidenced by the most recent exercise record. The awareness cycle is evidenced by the commissioning document. The email authentication record is measured against the register of exceptions. Testing covers the failure case, not only the happy path.

The email authentication record is reconciled with the register of exceptions. The segmentation boundary is evidenced by the quarterly review notes. The asset register is documented alongside the commissioning document. Testing covers the failure case, not only the happy path.

The physical controls is measured against the approved design baseline. The backup rotation is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Each administrative account is compared with the current written standard. The cloud baseline is compared with the previous year's assessment. The awareness cycle is traced to the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is validated by the previous year's assessment. The endpoint baseline is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The mobile standard is compared with the previous year's assessment. The encryption standard is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The risk register is measured against the most recent exercise record. The physical controls is reconciled with the quarterly review notes. The patch calendar is measured against the register of exceptions. The hardened build is compared with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.

The hardened build is traced to the evidence pack held by the owner. The third-party register is evidenced by the evidence pack held by the owner. The monitoring pipeline is checked against the approved design baseline. Every internet-facing service is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The metric set is documented alongside the approved design baseline. The remote access path 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 access review process is traced to the register of exceptions. The recovery test is validated by the evidence pack held by the owner. The remote access path is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

- Test result attached to the record.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The physical controls is validated by the agreed service level. The risk register is traced to the most recent exercise record. The segmentation boundary is reviewed against the approved design baseline. The physical controls is reviewed against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is compared with the ticket history for the period. The physical controls is reviewed against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

3. The threat model

The segmentation boundary is evidenced by the register of exceptions. The metric set is measured against the most recent exercise record. The physical controls is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

The vulnerability queue is evidenced by the evidence pack held by the owner. The classification scheme is traced to the previous year's assessment. Each administrative account is documented alongside the register of exceptions. The risk register is compared with the signed exception log. The control is tested at least once every twelve months.

The threat model is evidenced by the quarterly review notes. The continuity plan is validated by the evidence pack held by the owner. The hardened build is reconciled with the commissioning document. Testing covers the failure case, not only the happy path.

The privileged access list is reviewed against the agreed service level. The access review process is reconciled with the evidence pack held by the owner. The risk register is compared with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is checked against the quarterly review notes. The endpoint baseline is validated by the dependency map. The continuity plan is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The physical controls is traced to the commissioning document. The risk register is traced to the quarterly review notes. The hardened build is measured against the commissioning document. The hardened build is evidenced by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is compared with the current written standard. The endpoint baseline is traced to the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is reconciled with the register of exceptions. The email authentication record is reconciled with the register of exceptions. The metric set is reviewed against the previous year's assessment. The physical controls is checked against the ticket history for the period. Any deviation requires written approval and an expiry date.

The endpoint baseline is validated by the dependency map. The threat model is validated by the dependency map. The continuity plan is validated by the quarterly review notes. The recovery test is checked against the commissioning document. The intent is to make the safe path the default rather than an exception.

The continuity plan is documented alongside the signed exception log. The hardened build is validated by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The vendor register is documented alongside the evidence pack held by the owner. The change process is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is traced to the ticket history for the period. The encryption standard is compared with the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The mobile standard is evidenced by the previous year's assessment. The continuity plan is documented alongside the signed exception log. The retention schedule is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is compared with the dependency map. The segmentation boundary is measured against the signed exception log. The access review process is checked against the previous year's assessment. The backup rotation is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The threat model is reconciled with the approved design baseline. The email authentication record is measured against the previous year's assessment. The retention schedule is validated by the quarterly review notes. The email authentication record is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The vendor register is validated by the register of exceptions. The asset register is validated by the current written standard. The risk register is reviewed against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is measured against the signed exception log. The email authentication record is measured against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

- Test result attached to the record.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.

The threat model is checked against the ticket history for the period. The metric set is reconciled with the commissioning document. The procedure is written so a new starter can follow it without supervision.

The change process is validated by the commissioning document. The vendor register is checked against the quarterly review notes. The mobile standard is reviewed against the agreed service level. The identity lifecycle is measured against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is documented alongside the current written standard. The remote access path is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The endpoint baseline is evidenced by the previous year's assessment. Every internet-facing service is reviewed against the approved design baseline. The remote access path is documented alongside the quarterly review notes. The third-party register is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is traced to the current written standard. Each administrative account is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is reviewed against the evidence pack held by the owner. The awareness cycle is reconciled with the signed exception log. The monitoring pipeline is documented alongside the evidence pack held by the owner. The hardened build is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The threat model is evidenced by the approved design baseline. The segmentation boundary is compared with the approved design baseline. The hardened build is reconciled with the dependency map. Metrics are reported as trends rather than single data points.

4. The endpoint baseline

The physical controls is traced to the most recent exercise record. The email authentication record is reconciled with the register of exceptions. The asset register is documented alongside the evidence pack held by the owner. The metric set is measured against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The asset register is reconciled with the previous year's assessment. The backup rotation is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The classification scheme is evidenced by the signed exception log. The encryption standard is checked against the register of exceptions. The asset register is reviewed against the register of exceptions. The awareness cycle is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

The retention schedule is documented alongside the evidence pack held by the owner. The encryption standard is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is compared with the current written standard. The backup rotation is checked against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reviewed against the dependency map. The retention schedule is documented alongside the most recent exercise record. The recovery test is documented alongside the most recent exercise record. The third-party register is documented alongside the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is compared with the signed exception log. The monitoring pipeline is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

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

The segmentation boundary is evidenced by the register of exceptions. The retention schedule is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is reconciled with the previous year's assessment. The asset register is validated by the previous year's assessment. The endpoint baseline is documented alongside the commissioning document. The risk register is compared with the commissioning document. Testing covers the failure case, not only the happy path.

The segmentation boundary is compared with the register of exceptions. The retention schedule is traced to the commissioning document. The asset register is reconciled with the evidence pack held by the owner. The recovery test is documented alongside the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The physical controls is compared with the evidence pack held by the owner. The patch calendar is documented alongside the previous year's assessment. The hardened build is checked against the most recent exercise record. Records are retained only as long as the schedule requires.

The vendor register is measured against the most recent exercise record. The classification scheme is validated by the current written standard. The vendor register 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 third-party register is checked against the ticket history for the period. The privileged access list is evidenced by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is checked against the current written standard. The third-party register is compared with the agreed service level. Records are retained only as long as the schedule requires.

5. The metric set

The change process is reconciled with the agreed service level. The email authentication record is measured against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reconciled with the register of exceptions. The classification scheme is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is evidenced by the quarterly review notes. The privileged access list is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

The email authentication record is reviewed against the ticket history for the period. The change process is reconciled with the current written standard. Evidence is kept for audit, insurance and regulator requests.