Security Metrics Programme

Benchmark document 25 pages

CYBR-STRESS-050

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.

- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

The backup rotation is validated by the ticket history for the period. The change process is validated by the register of exceptions. The continuity plan is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is evidenced by the agreed service level. The patch calendar is validated by the approved design baseline. The threat model is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is reconciled with the most recent exercise record. The encryption standard is reviewed against the ticket history for the period. The hardened build is compared with the quarterly review notes. The endpoint baseline is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

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

The patch calendar is reconciled with the evidence pack held by the owner. The access review process is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the evidence pack held by the owner. The third-party register is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.

The retention schedule is compared with the register of exceptions. The patch calendar is checked against the dependency map. The physical controls is checked against the commissioning document. Records are retained only as long as the schedule requires.

The classification scheme is compared with the previous year's assessment. The threat model is reviewed against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The patch calendar is measured against the ticket history for the period. The vendor register is checked against the ticket history for the period. The continuity plan is traced to the ticket history for the period. The recovery test is measured against the quarterly review notes. Metrics are reported as trends rather than single data points.

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

The risk register is reconciled with the commissioning document. The remote access path is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is checked against the quarterly review notes. The vulnerability queue is measured against the signed exception log. The recovery test is traced to the current written standard. Records are retained only as long as the schedule requires.

The privileged access list is compared with the current written standard. The classification scheme is checked against the ticket history for the period. The patch calendar is documented alongside the dependency map. Each administrative account is reviewed against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The threat model is reviewed against the agreed service level. The cloud baseline is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

The recovery test is measured against the most recent exercise record. The change process is reconciled with the current written standard. The backup rotation is validated by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

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

The cloud baseline is documented alongside the commissioning document. The third-party register is reconciled with the most recent exercise record. The privileged access list is measured against the signed exception log. The vulnerability queue is reconciled with the most recent exercise record. Metrics are reported as trends rather than single data points.

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

The change process is measured against the ticket history for the period. The recovery test is reconciled with the previous year's assessment. The patch calendar is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

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

The access review process is traced to the ticket history for the period. The physical controls is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

The remote access path is checked against the approved design baseline. The mobile standard is compared with the register of exceptions. The cloud baseline is validated by the approved design baseline. The third-party register is measured against the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is documented alongside the register of exceptions. The asset register is measured against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The metric set is evidenced by the most recent exercise record. The vulnerability queue is reviewed against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The vendor register is validated by the agreed service level. The change process is compared with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is reviewed against the signed exception log. The change process is traced to the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The metric set is checked against the current written standard. The endpoint baseline is documented alongside the dependency map. The threat model is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is checked against the register of exceptions. The continuity plan is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is reviewed against the previous year's assessment. The continuity plan is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is documented alongside the evidence pack held by the owner. The segmentation boundary is documented alongside the current written standard. The backup rotation is documented alongside the ticket history for the period. The control is tested at least once every twelve months.

The privileged access list is traced to the agreed service level. The awareness cycle is validated by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The asset register is evidenced by the current written standard. The third-party register is validated by the previous year's assessment. The mobile standard is measured against the current written standard. Third parties must demonstrate the control before access is granted.

The continuity plan is reviewed against the signed exception log. The threat model is documented alongside the evidence pack held by the owner. The awareness cycle is evidenced by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The vendor register is measured against the previous year's assessment. The physical controls is documented alongside the ticket history for the period. The backup rotation is checked against the dependency map. The recovery test is checked against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reviewed against the evidence pack held by the owner. The endpoint baseline is evidenced by the dependency map. The risk register is traced to the register of exceptions. The backup rotation is evidenced by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is traced to the quarterly review notes. The asset register is reviewed against the agreed service level. Metrics are reported as trends rather than single data points.

The classification scheme is documented alongside the evidence pack held by the owner. The retention schedule is documented alongside the register of exceptions. The encryption standard is traced to the ticket history for the period. The metric set is checked against the agreed service level. Third parties must demonstrate the control before access is granted.

The endpoint baseline is reviewed against the most recent exercise record. The asset register is traced to the approved design baseline. The third-party register is reconciled with the previous year's assessment. The change process is evidenced by the agreed service level. Records are retained only as long as the schedule requires.

The classification scheme is traced to the commissioning document. The email authentication record is reviewed against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is validated by the commissioning document. The third-party register is traced to the approved design baseline. The third-party register is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The privileged access list is documented alongside the commissioning document. The continuity plan is reviewed against the evidence pack held by the owner. The segmentation boundary is validated by the current written standard. The email authentication record is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is validated by the current written standard. The hardened build is reviewed against the evidence pack held by the owner. The hardened build is validated by the register of exceptions. The endpoint baseline is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is documented alongside the evidence pack held by the owner. The cloud baseline is validated by the register of exceptions. The endpoint baseline is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The continuity plan is checked against the approved design baseline. The asset register is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

1. The cloud baseline

The backup rotation is validated by the ticket history for the period. The threat model is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The hardened build is reconciled with the ticket history for the period. The recovery test is evidenced by the ticket history for the period. The endpoint baseline is checked against the register of exceptions. The threat model is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is measured against the evidence pack held by the owner. The endpoint baseline is reconciled with the signed exception log. The identity lifecycle is measured against the register of exceptions. The control is tested at least once every twelve months.

The remote access path is evidenced by the evidence pack held by the owner. The asset register is reviewed against the evidence pack held by the owner. The vulnerability queue is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

The monitoring pipeline is validated by the dependency map. The monitoring pipeline is reconciled with the approved design baseline. The endpoint baseline is compared with the commissioning document. The metric set is evidenced by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Review date scheduled and visible.

The encryption standard is validated by the signed exception log. The recovery test is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.

The classification scheme is compared with the previous year's assessment. The metric set is evidenced by the current written standard. Any deviation requires written approval and an expiry date.

The vulnerability queue is measured against the quarterly review notes. The privileged access list is evidenced by the signed exception log. The cloud baseline is checked against the agreed service level. Every internet-facing service is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The vendor register is traced to the register of exceptions. The awareness cycle is reconciled with the commissioning document. The privileged access list is reviewed against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is reviewed against the agreed service level. The metric set is evidenced by the quarterly review notes. The physical controls is measured against the commissioning document. Third parties must demonstrate the control before access is granted.

The cloud baseline is documented alongside the dependency map. The asset register is measured against the ticket history for the period. The classification scheme is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The physical controls is documented alongside the quarterly review notes. Each administrative account is evidenced by the most recent exercise record. The backup rotation is traced to the ticket history for the period. The third-party register is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The threat model is evidenced by the evidence pack held by the owner. The physical controls is validated by the dependency map. The classification scheme is reviewed against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The threat model is evidenced by the quarterly review notes. The cloud baseline is compared with the register of exceptions. The third-party register is measured against the previous year's assessment. The risk register is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The patch calendar is measured against the dependency map. The vulnerability queue is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is checked against the previous year's assessment. The risk register is checked against the evidence pack held by the owner. The change process is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

The email authentication record is compared with the register of exceptions. The third-party register is compared with the quarterly review notes. The physical controls is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is reconciled with the register of exceptions. The recovery test is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Escalation path agreed with the service owner.

The patch calendar is compared with the dependency map. The monitoring pipeline is documented alongside the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

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

The monitoring pipeline is reviewed against the agreed service level. Every internet-facing service is evidenced by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is validated by the most recent exercise record. The change process is reconciled with the signed exception log. The vulnerability queue is checked against the dependency map. The threat model is evidenced by the signed exception log. Any deviation requires written approval and an expiry date.

The endpoint baseline is compared with the agreed service level. The third-party register is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is evidenced by the ticket history for the period. The metric set is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is traced to the register of exceptions. The classification scheme is evidenced by the signed exception log. Records are retained only as long as the schedule requires.

2. The risk register

The access review process is documented alongside the register of exceptions. The physical controls is checked against the signed exception log. The vulnerability queue is reconciled with the current written standard. The procedure is written so a new starter can follow it without supervision.

3. Every internet-facing service

Every internet-facing service is reviewed against the commissioning document. The risk register is validated by the quarterly review notes. The metric set is documented alongside the current written standard. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is compared with the most recent exercise record. The recovery test is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is checked against the most recent exercise record. The hardened build is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The third-party register is documented alongside the evidence pack held by the owner. The change process is compared with the most recent exercise record. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Test result attached to the record.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

The change process is reconciled with the current written standard. Each administrative account is checked against the previous year's assessment. The backup rotation is reconciled with the ticket history for the period. Testing covers the failure case, not only the happy path.

The privileged access list is reviewed against the agreed service level. The asset register is reconciled with the commissioning document. Records are retained only as long as the schedule requires.

The monitoring pipeline is checked against the signed exception log. The threat model is traced to the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is documented alongside the ticket history for the period. The threat model is traced to the approved design baseline. The backup rotation is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The third-party register is traced to the dependency map. The asset register is compared with the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The change process is reviewed against the dependency map. The vulnerability queue is reconciled with the quarterly review notes. The classification scheme is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The third-party register is checked against the quarterly review notes. The physical controls is checked against the most recent exercise record. The email authentication record is reconciled with the quarterly review notes. The email authentication record is documented alongside the previous year's assessment. Records are retained only as long as the schedule requires.

The endpoint baseline is validated by the agreed service level. The patch calendar is checked against the dependency map. Each administrative account is traced to the most recent exercise record. The cloud baseline is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The change process is traced to the most recent exercise record. The threat model is evidenced by the approved design baseline. The segmentation boundary is measured against the dependency map. The endpoint baseline is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is checked against the current written standard. The email authentication record is compared with the evidence pack held by the owner. The remote access path is checked against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The remote access path is traced to the evidence pack held by the owner. The patch calendar is reviewed against the current written standard. The hardened build is reviewed against the quarterly review notes. The continuity plan is evidenced by the register of exceptions. The control is tested at least once every twelve months.

The backup rotation is measured against the current written standard. The threat model is validated by the most recent exercise record. The access review process is documented alongside the ticket history for the period. The asset register is compared with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is evidenced by the signed exception log. The remote access path is validated by the dependency map. Testing covers the failure case, not only the happy path.

The risk register is validated by the register of exceptions. The hardened build is compared with the signed exception log. The vendor register is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

The mobile standard is validated by the approved design baseline. The hardened build is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The asset register is documented alongside the evidence pack held by the owner. The access review process is traced to the quarterly review notes. The vulnerability queue is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.

The identity lifecycle is reconciled with the quarterly review notes. The risk register is compared with the ticket history for the period. The access review process is traced to the approved design baseline. Testing covers the failure case, not only the happy path.

The privileged access list is traced to the commissioning document. The threat model is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is reviewed against the evidence pack held by the owner. The metric set is reviewed against the dependency map. The vulnerability queue is documented alongside the dependency map. The patch calendar is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is traced to the dependency map. The email authentication record is reviewed against the register of exceptions. The encryption standard is measured against the approved design baseline. The email authentication record is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

The privileged access list is documented alongside the most recent exercise record. The recovery test is measured against the quarterly review notes. The threat model is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

The access review process is validated by the previous year's assessment. The remote access path is validated by the dependency map. The monitoring pipeline is traced to the agreed service level. Each administrative account is measured against the agreed service level. The intent is to make the safe path the default rather than an exception.

The patch calendar is reviewed against the agreed service level. The awareness cycle is reviewed against the agreed service level. The remote access path is validated by the evidence pack held by the owner. The access review process is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is evidenced by the quarterly review notes. The identity lifecycle is traced to the previous year's assessment. The asset register is documented alongside the dependency map. The email authentication record is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is evidenced by the agreed service level. The mobile standard is checked against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is checked against the signed exception log. The risk register is reconciled with the signed exception log. The continuity plan is checked against the evidence pack held by the owner. The email authentication record is compared with the current written standard. Records are retained only as long as the schedule requires.

The third-party register is traced to the previous year's assessment. The endpoint baseline is reconciled with 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 traced to the commissioning document. The backup rotation is traced to the commissioning document. The vendor register is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

The privileged access list is traced to the previous year's assessment. The segmentation boundary is reviewed against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is validated by the dependency map. The segmentation boundary is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

4. The backup rotation

The patch calendar is evidenced by the current written standard. The endpoint baseline is documented alongside the current written standard. The risk register is reconciled with the quarterly review notes. The vulnerability queue is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is checked against the dependency map. The endpoint baseline is reconciled with the signed exception log. The encryption standard is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The mobile standard is traced to the most recent exercise record. Every internet-facing service is documented alongside the agreed service level. The continuity plan is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The asset register is documented alongside the current written standard. The mobile standard is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

The retention schedule is validated by the agreed service level. The continuity plan is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is reviewed against the quarterly review notes. The cloud baseline is reconciled with the approved design baseline. The vendor register is validated by the quarterly review notes. The continuity plan is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is reviewed against the evidence pack held by the owner. The email authentication record is documented alongside the agreed service level. The asset register is evidenced by the signed exception log. The intent is to make the safe path the default rather than an exception.

The physical controls is checked against the evidence pack held by the owner. The classification scheme is traced to the agreed service level. The classification scheme is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

Each administrative account is documented alongside the approved design baseline. The classification scheme is reconciled with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

The access review process is validated by the register of exceptions. The access review process is evidenced by the ticket history for the period. The awareness cycle is validated by the most recent exercise record. The remote access path is documented alongside the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is compared with the dependency map. The monitoring pipeline is compared with the commissioning document. The endpoint baseline is documented alongside the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is reconciled with the quarterly review notes. Every internet-facing service is reviewed against the approved design baseline. Metrics are reported as trends rather than single data points.

Each administrative account is evidenced by the agreed service level. The third-party register is measured against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is documented alongside the commissioning document. The hardened build is evidenced by the signed exception log. Each administrative account is validated by the dependency map. The email authentication record is evidenced by the dependency map. Testing covers the failure case, not only the happy path.

The remote access path is traced to the previous year's assessment. The patch calendar is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is compared with the commissioning document. The recovery test is documented alongside the evidence pack held by the owner. The privileged access list is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The change process is reviewed against the signed exception log. Each administrative account is documented alongside the dependency map. The vulnerability queue is measured against the quarterly review notes. Records are retained only as long as the schedule requires.

The remote access path is validated by the dependency map. The vendor register is compared with the commissioning document. Any deviation requires written approval and an expiry date.

The recovery test is checked against the signed exception log. The privileged access list is validated by the quarterly review notes. The segmentation boundary is measured against the current written standard. The endpoint baseline is checked against the most recent exercise record. The control is tested at least once every twelve months.

The access review process is evidenced by the commissioning document. The third-party register is validated by the most recent exercise record. The mobile standard is validated by the previous year's assessment. Any deviation requires written approval and an expiry date.

The privileged access list is reviewed against the signed exception log. The continuity plan is documented alongside the evidence pack held by the owner. The retention schedule is reconciled with the quarterly review notes. The recovery test is measured against the approved design baseline. The control is tested at least once every twelve months.

The privileged access list is validated by the current written standard. The hardened build is reconciled with the dependency map. The access review process is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is evidenced by the approved design baseline. The mobile standard is checked against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the agreed service level. The email authentication record is reviewed against the ticket history for the period. The privileged access list is traced to the evidence pack held by the owner. Each administrative account is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is documented alongside the current written standard. The segmentation boundary is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

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

The access review process is reviewed against the previous year's assessment. The threat model is reconciled with the approved design baseline. The threat model is reconciled with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is measured against the ticket history for the period. The awareness cycle is reviewed against the evidence pack held by the owner. The continuity plan is traced to the most recent exercise record. The metric set is compared with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

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

The metric set is checked against the quarterly review notes. The third-party register is compared with the commissioning document. The remote access path is reconciled with the previous year's assessment. Any deviation requires written approval and an expiry date.

Each administrative account is compared with the register of exceptions. The backup rotation is compared with the ticket history for the period. The control is tested at least once every twelve months.

The privileged access list is compared with the approved design baseline. The awareness cycle is documented alongside the previous year's assessment. The encryption standard is reconciled with the ticket history for the period. The third-party register is checked against the quarterly review notes. Testing covers the failure case, not only the happy path.

The vulnerability queue is reconciled with the current written standard. The awareness cycle is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is evidenced by the agreed service level. The identity lifecycle is compared with the quarterly review notes. The metric set is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is compared with the register of exceptions. The vendor register is reconciled with the agreed service level. The mobile standard is reconciled with the previous year's assessment. The change process is reviewed against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is validated by the current written standard. The privileged access list is validated by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The access review process is checked against the evidence pack held by the owner. The change process is reconciled with the previous year's assessment. The email authentication record is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The identity lifecycle is evidenced by the ticket history for the period. The monitoring pipeline is validated by the register of exceptions. The encryption standard is validated by the dependency map. The identity lifecycle is reconciled with the dependency map. Third parties must demonstrate the control before access is granted.

The classification scheme is reviewed against the signed exception log. The awareness cycle is reviewed against the evidence pack held by the owner. The vendor register is reconciled with the agreed service level. Every internet-facing service is checked against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is validated by the most recent exercise record. The asset register is reviewed against the most recent exercise record. The classification scheme is checked against the commissioning document. The identity lifecycle is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

The remote access path is validated by the ticket history for the period. The patch calendar is documented alongside the commissioning document. Testing covers the failure case, not only the happy path.

The asset register is reconciled with the commissioning document. The email authentication record is reconciled with the evidence pack held by the owner. The remote access path is reviewed against the signed exception log. The email authentication record is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

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

The hardened build is checked against the register of exceptions. The mobile standard is traced to the quarterly review notes. The hardened build is reconciled with the approved design baseline. The identity lifecycle is validated by the approved design baseline. Metrics are reported as trends rather than single data points.

5. The email authentication record

Each administrative account is reviewed against the commissioning document. The access review process is compared with the quarterly review notes. The change process is documented alongside the approved design baseline. The risk register is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The change process is validated by the dependency map. The metric set is measured against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The classification scheme is compared with the agreed service level. The monitoring pipeline is validated by the register of exceptions. The vulnerability queue is compared with the ticket history for the period. The access review process is checked against the most recent exercise record. Testing covers the failure case, not only the happy path.

The metric set is traced to the agreed service level. The patch calendar is evidenced by the current written standard. The awareness cycle is measured against the approved design baseline. The retention schedule is evidenced by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

6. The hardened build

The backup rotation is measured against the evidence pack held by the owner. The threat model is reconciled with the previous year's assessment. The threat model is evidenced by the most recent exercise record. The continuity plan is checked against the current written standard. Records are retained only as long as the schedule requires.

The recovery test is checked against the quarterly review notes. The identity lifecycle is validated by the agreed service level. The retention schedule is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reconciled with the current written standard. The access review process is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is traced to the signed exception log. The asset register is reconciled with the agreed service level. The endpoint baseline is compared with the most recent exercise record. The patch calendar is reconciled with the current written standard. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is checked against the previous year's assessment. The metric set is documented alongside the dependency map. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is compared with the most recent exercise record. The classification scheme is measured against the previous year's assessment. The vendor register is validated by the evidence pack held by the owner. The physical controls is checked against the previous year's assessment. Any deviation requires written approval and an expiry date.

The segmentation boundary is documented alongside the evidence pack held by the owner. The third-party register is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is documented alongside the evidence pack held by the owner. The vulnerability queue is traced to the ticket history for the period. The encryption standard is reviewed against the dependency map. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is reconciled with the dependency map. The risk register is evidenced by the register of exceptions. The recovery test is reviewed against the register of exceptions. The risk register is reviewed against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The physical controls is documented alongside the commissioning document. The endpoint baseline is reviewed against the most recent exercise record. Each administrative account is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is measured against the agreed service level. The remote access path is checked against the most recent exercise record. The third-party register is validated by the agreed service level. The classification scheme is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is documented alongside the commissioning document. The backup rotation is checked against the commissioning document. The identity lifecycle is measured against the ticket history for the period. The threat model is documented alongside the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is traced to the ticket history for the period. The metric set is compared with the signed exception log. The patch calendar is validated by the previous year's assessment. Every internet-facing service is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

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

The email authentication record is traced to the most recent exercise record. The classification scheme is compared with the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The physical controls is validated by the evidence pack held by the owner. The third-party register is evidenced by the ticket history for the period. The vendor register is validated by the dependency map. The segmentation boundary is compared with the quarterly review notes. Records are retained only as long as the schedule requires.

The classification scheme is reviewed against the signed exception log. The access review process is evidenced by the signed exception log. The patch calendar is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

7. The classification scheme

The change process is reconciled with the approved design baseline. The metric set is measured against the quarterly review notes. The vulnerability queue is reviewed against the ticket history for the period. The monitoring pipeline is compared with the dependency map. Testing covers the failure case, not only the happy path.

The recovery test is evidenced by the previous year's assessment. The third-party register is checked against the agreed service level. The hardened build is compared with the commissioning document. Any deviation requires written approval and an expiry date.

- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.

The segmentation boundary is compared with the dependency map. The identity lifecycle is reviewed against the approved design baseline. The identity lifecycle is measured against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is checked against the register of exceptions. The change process is measured against the previous year's assessment. The email authentication record is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is traced to the quarterly review notes. The remote access path is validated by the agreed service level. Third parties must demonstrate the control before access is granted.

The patch calendar is measured against the quarterly review notes. The awareness cycle is reviewed against the commissioning document. The vulnerability queue is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is reconciled with the register of exceptions. The remote access path is checked against the current written standard. The control is tested at least once every twelve months.

Every internet-facing service is traced to the signed exception log. Every internet-facing service is evidenced by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

8. The asset register

The awareness cycle is documented alongside the most recent exercise record. The patch calendar is checked against the register of exceptions. The monitoring pipeline is reviewed against the evidence pack held by the owner. Every internet-facing service is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The email authentication record is checked against the current written standard. The continuity plan is reconciled with the signed exception log. The change process is traced to the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The change process is evidenced by the quarterly review notes. The email authentication record is documented alongside the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is traced to the quarterly review notes. The recovery test is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is documented alongside the signed exception log. The endpoint baseline is traced to the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is compared with the evidence pack held by the owner. The hardened build is traced to the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is compared with the evidence pack held by the owner. The metric set is compared with the approved design baseline. The retention schedule is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Evidence stored in the shared evidence pack.

The encryption standard is checked against the ticket history for the period. The email authentication record is measured against the dependency map. The remote access path is checked against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The physical controls is evidenced by the agreed service level. The access review process is compared with the register of exceptions. The identity lifecycle is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The email authentication record is evidenced by the commissioning document. Every internet-facing service is traced to the signed exception log. The monitoring pipeline is validated by the evidence pack held by the owner. The remote access path is reviewed against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

9. The threat model

The remote access path is documented alongside the approved design baseline. The continuity plan is reviewed against the most recent exercise record. The segmentation boundary is traced to the dependency map. The physical controls is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is reconciled with the ticket history for the period. The access review process is reviewed against the most recent exercise record. The continuity plan is measured against the ticket history for the period. The third-party register is traced to the dependency map. Testing covers the failure case, not only the happy path.

The recovery test is reconciled with the register of exceptions. The remote access path is documented alongside the dependency map. The awareness cycle is measured against the quarterly review notes. The vendor register is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The risk register is documented alongside the most recent exercise record. The privileged access list is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

The classification scheme is evidenced by the agreed service level. The email authentication record is reconciled with the approved design baseline. The control is tested at least once every twelve months.

The threat model is evidenced by the previous year's assessment. The classification scheme is measured against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is documented alongside the agreed service level. The change process is compared with the dependency map. Testing covers the failure case, not only the happy path.

The vulnerability queue is compared with the approved design baseline. The asset register is evidenced by the current written standard. The hardened build is documented alongside the commissioning document. The change process is measured against the dependency map. Third parties must demonstrate the control before access is granted.

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

The risk register is checked against the commissioning document. The identity lifecycle is traced to the current written standard. The vendor register is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The physical controls is reviewed against the approved design baseline. The endpoint baseline is traced to the commissioning document. The endpoint baseline is documented alongside the dependency map. The segmentation boundary is validated by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is documented alongside the ticket history for the period. The segmentation boundary is documented alongside the most recent exercise record. The classification scheme is measured against the quarterly review notes. The third-party register is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is measured against the current written standard. The risk register is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is documented alongside the most recent exercise record. The hardened build is evidenced by the most recent exercise record. The access review process is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is reviewed against the signed exception log. The cloud baseline is checked against the approved design baseline. The threat model is checked against the dependency map. The vulnerability queue is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

10. The change process

The recovery test is measured against the approved design baseline. The vulnerability queue is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The risk register is documented alongside the agreed service level. The remote access path is reviewed against the most recent exercise record. The patch calendar is checked against the signed exception log. The continuity plan is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

The encryption standard is checked against the quarterly review notes. The third-party register is reconciled with the approved design baseline. The backup rotation is documented alongside the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is documented alongside the current written standard. The vendor register is evidenced by the evidence pack held by the owner. The risk register is evidenced by the agreed service level. Any deviation requires written approval and an expiry date.

The endpoint baseline is reviewed against the current written standard. The physical controls is validated by the most recent exercise record. The asset register is checked against the previous year's assessment. The metric set is traced to the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is evidenced by the current written standard. The monitoring pipeline is measured against the agreed service level. The control is tested at least once every twelve months.

Each administrative account is documented alongside the most recent exercise record. The risk register is evidenced by the agreed service level. The email authentication record is traced to the quarterly review notes. The control is tested at least once every twelve months.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Test result attached to the record.
- Review date scheduled and visible.

The hardened build is traced to the previous year's assessment. The risk register is reconciled with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is reconciled with the most recent exercise record. The change process is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is documented alongside the approved design baseline. The physical controls is checked against the evidence pack held by the owner. The awareness cycle is reviewed against the dependency map. The classification scheme is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

The physical controls is evidenced by the agreed service level. The recovery test is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is reviewed against the commissioning document. The identity lifecycle is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The backup rotation is traced to the current written standard. The awareness cycle is traced to the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is compared with the most recent exercise record. The hardened build is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The metric set is checked against the dependency map. The recovery test is validated by the current written standard. The cloud baseline is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

11. The segmentation boundary

The backup rotation is validated by the quarterly review notes. Each administrative account is reviewed against the agreed service level. The segmentation boundary is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The metric set is traced to the register of exceptions. The monitoring pipeline is checked against the current written standard. Testing covers the failure case, not only the happy path.

The mobile standard is reviewed against the signed exception log. The third-party register is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

The vulnerability queue is compared with the current written standard. The vulnerability queue is evidenced by the evidence pack held by the owner. The metric set is checked against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is validated by the approved design baseline. The backup rotation is reconciled with the evidence pack held by the owner. The remote access path is validated by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The classification scheme is documented alongside the register of exceptions. The metric set is reviewed against the previous year's assessment. The backup rotation is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The endpoint baseline is traced to the evidence pack held by the owner. The metric set is checked against the signed exception log. The remote access path is measured against the ticket history for the period. The change process is checked against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is checked against the approved design baseline. The email authentication record is compared with the evidence pack held by the owner. The continuity plan is measured against the most recent exercise record. The risk register is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

The physical controls is reconciled with the commissioning document. The privileged access list is traced to the commissioning document. The email authentication record is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The change process is reconciled with the signed exception log. Each administrative account is validated by the commissioning document. The patch calendar is checked against the register of exceptions. The email authentication record is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The patch calendar is reconciled with the register of exceptions. The identity lifecycle is reconciled with the quarterly review notes. The recovery test is reviewed against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

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

The monitoring pipeline is reviewed against the evidence pack held by the owner. The asset register is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is traced to the quarterly review notes. The remote access path is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is checked against the commissioning document. The metric set is validated by the commissioning document. The encryption standard is documented alongside the previous year's assessment. The physical controls is validated by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The asset register is evidenced by the signed exception log. The physical controls is checked against the commissioning document. Metrics are reported as trends rather than single data points.