Phishing Simulation Runbook

Exercise record 25 pages

CYBR-STRESS-089

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

The third-party register is validated by the signed exception log. The asset register is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The metric set is reconciled with the agreed service level. The hardened build is reconciled with the dependency map. Every internet-facing service is compared with the dependency map. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is traced to the register of exceptions. The vulnerability queue is measured against the register of exceptions. The threat model is evidenced by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is reviewed against the signed exception log. The email authentication record is compared with the commissioning document. The cloud baseline is measured against the signed exception log. 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 vulnerability queue is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is validated by the dependency map. The continuity plan is reviewed against the commissioning document. The backup rotation is measured against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is documented alongside the agreed service level. The awareness cycle is evidenced by the agreed service level. The vendor register is traced to the evidence pack held by the owner. The identity lifecycle is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

The vendor register is traced to the agreed service level. The recovery test is measured against the commissioning document. The retention schedule is compared with the evidence pack held by the owner. The segmentation boundary is compared with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The recovery test is documented alongside the quarterly review notes. The identity lifecycle is validated by the evidence pack held by the owner. The third-party register is compared with the commissioning document. The classification scheme is measured against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is reviewed against the commissioning document. The segmentation boundary is traced to the dependency map. Third parties must demonstrate the control before access is granted.

The physical controls is reviewed against the previous year's assessment. The mobile standard is checked against the signed exception log. The continuity plan is documented alongside the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The access review process is measured against the dependency map. The hardened build is compared with the ticket history for the period. The endpoint baseline is validated by the current written standard. The patch calendar is compared with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

1. The physical controls

The retention schedule is measured against the dependency map. The recovery test is compared with the approved design baseline. The remote access path is documented alongside the quarterly review notes. The identity lifecycle is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The remote access path is compared with the most recent exercise record. The access review process is traced to the commissioning document. The mobile standard is reviewed against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is evidenced by the ticket history for the period. The access review process is documented alongside the agreed service level. The control is tested at least once every twelve months.

The vulnerability queue is evidenced by the agreed service level. The asset register is checked against the commissioning document. The monitoring pipeline is compared with the ticket history for the period. The recovery test is documented alongside the signed exception log. Any deviation requires written approval and an expiry date.

The hardened build is compared with the ticket history for the period. The email authentication record is compared with the agreed service level. The asset register is measured against the approved design baseline. The intent is to make the safe path the default rather than an exception.

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

The identity lifecycle is measured against the dependency map. The physical controls is checked against the previous year's assessment. The continuity plan is checked against the current written standard. The classification scheme is measured against the agreed service level. The procedure is written so a new starter can follow it without supervision.

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

The retention schedule is reviewed against the current written standard. The change process is validated by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The physical controls is reviewed against the ticket history for the period. The vendor register is reviewed against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is traced to the previous year's assessment. The physical controls is evidenced by the commissioning document. The access review process is compared with the dependency map. The access review process is evidenced by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is checked against the register of exceptions. Every internet-facing service is reviewed against the commissioning document. The awareness cycle is reviewed against the signed exception log. The privileged access list is reconciled with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The encryption standard is checked against the evidence pack held by the owner. The encryption standard is measured against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is checked against the dependency map. The cloud baseline is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

The vulnerability queue is reviewed against the register of exceptions. The segmentation boundary is compared with the current written standard. Third parties must demonstrate the control before access is granted.

The mobile standard is measured 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 agreed service level. The encryption standard is documented alongside the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The risk register is reconciled with the agreed service level. The access review process is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The vendor register is compared with the register of exceptions. The change process is traced to the quarterly review notes. The endpoint baseline is reconciled with the agreed service level. The control is tested at least once every twelve months.

The vendor register is documented alongside the register of exceptions. The risk register is evidenced by the dependency map. The endpoint baseline is documented alongside the ticket history for the period. Third parties must demonstrate the control before access is granted.

The classification scheme is reconciled with the most recent exercise record. The identity lifecycle is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The remote access path is measured against the quarterly review notes. The email authentication record is checked against the previous year's assessment. The awareness cycle is measured against the evidence pack held by the owner. The identity lifecycle is checked against the current written standard. Metrics are reported as trends rather than single data points.

The vulnerability queue is validated by the current written standard. The classification scheme is evidenced by the current written standard. Every internet-facing service is documented alongside the previous year's assessment. The segmentation boundary is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

The remote access path is validated by the signed exception log. Every internet-facing service is compared with the current written standard. Metrics are reported as trends rather than single data points.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Acceptance criteria written before work starts.

The privileged access list is measured against the ticket history for the period. The risk register is checked against the previous year's assessment. The change process is compared with the quarterly review notes. The metric set is evidenced by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is validated by the approved design baseline. The continuity plan is measured against the commissioning document. Every internet-facing service is traced to the current written standard. The awareness cycle is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is traced to the previous year's assessment. The cloud baseline is measured against the agreed service level. The continuity plan 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 third-party register is compared with the current written standard. The identity lifecycle is measured against the agreed service level. The remote access path is checked against the commissioning document. Every internet-facing service is traced to the current written standard. The control is tested at least once every twelve months.

The third-party register is compared with the quarterly review notes. The cloud baseline is reconciled with the evidence pack held by the owner. The endpoint baseline is reconciled with the register of exceptions. The cloud baseline is checked against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is checked against the ticket history for the period. The endpoint baseline is reviewed against the quarterly review notes. The identity lifecycle is documented alongside the signed exception log. The vulnerability queue is compared with the signed exception log. The control is tested at least once every twelve months.

The change process is reconciled with the commissioning document. The email authentication record is evidenced by the ticket history for the period. The vendor register is evidenced by the current written standard. The segmentation boundary is checked against the register of exceptions. Records are retained only as long as the schedule requires.

The vulnerability queue is documented alongside the most recent exercise record. The backup rotation is measured against the register of exceptions. The vulnerability queue is evidenced by the dependency map. The asset register is documented alongside the ticket history for the period. The control is tested at least once every twelve months.

The email authentication record is reviewed against the commissioning document. The recovery test is compared with the current written standard. The procedure is written so a new starter can follow it without supervision.

The remote access path is evidenced by the dependency map. The encryption standard is traced to the most recent exercise record. The classification scheme is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The threat model is validated by the dependency map. The monitoring pipeline is compared with the dependency map. Testing covers the failure case, not only the happy path.

The continuity plan is compared with the current written standard. The hardened build is reviewed against the evidence pack held by the owner. The segmentation boundary is checked against the commissioning document. Third parties must demonstrate the control before access is granted.

3. The cloud baseline

The cloud baseline is reviewed against the previous year's assessment. The remote access path is traced to the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is compared with the current written standard. The backup rotation is compared with the quarterly review notes. The segmentation boundary is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is measured against the current written standard. Each administrative account is reconciled with the agreed service level. Each administrative account is validated by the most recent exercise record. The change process is compared with the register of exceptions. Testing covers the failure case, not only the happy path.

The privileged access list is validated by the current written standard. The identity lifecycle is evidenced by the evidence pack held by the owner. The hardened build is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

The segmentation boundary is reconciled with the approved design baseline. The change process is compared with the previous year's assessment. The remote access path is evidenced by the register of exceptions. Each administrative account is compared with the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is reviewed against the current written standard. The continuity plan is traced to the current written standard. The privileged access list is traced to the evidence pack held by the owner. The privileged access list is traced to the quarterly review notes. Any deviation requires written approval and an expiry date.

The monitoring pipeline is reconciled with the commissioning document. The encryption standard is reconciled with the commissioning document. The asset register is compared with the dependency map. The remote access path is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The awareness cycle is traced to the signed exception log. The encryption standard is compared with the evidence pack held by the owner. The risk register is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is reviewed against the approved design baseline. The classification scheme is checked against the most recent exercise record. The continuity plan is documented alongside the most recent exercise record. The remote access path is evidenced by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

4. The threat model

The metric set is reviewed against the ticket history for the period. The identity lifecycle is compared with the approved design baseline. The continuity plan is reviewed against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is compared with the quarterly review notes. The asset register is reviewed against the most recent exercise record. The mobile standard is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is checked against the quarterly review notes. The awareness cycle is reconciled with the dependency map. The physical controls is reviewed against the commissioning document. Metrics are reported as trends rather than single data points.

The vendor register is checked against the commissioning document. The access review process is documented alongside the most recent exercise record. The patch calendar is measured against the most recent exercise record. The retention schedule is measured against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is compared with the signed exception log. The retention schedule is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

The asset register is measured against the previous year's assessment. The backup rotation is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

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

The monitoring pipeline is measured against the approved design baseline. The endpoint baseline is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

5. The identity lifecycle

The vendor register is reviewed against the evidence pack held by the owner. The retention schedule is documented alongside the current written standard. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is reconciled with the dependency map. The segmentation boundary is evidenced by the current written standard. The threat model is evidenced by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The asset register is traced to the approved design baseline. The classification scheme is reconciled with the current written standard. The threat model is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is documented alongside the agreed service level. The patch calendar is compared with the approved design baseline. Any deviation requires written approval and an expiry date.

The access review process is reviewed against the quarterly review notes. The remote access path is evidenced by the agreed service level. The vulnerability queue is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The threat model is checked against the current written standard. Every internet-facing service is reconciled with the agreed service level. The email authentication record is compared with the most recent exercise record. Every internet-facing service is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

6. The cloud baseline

The third-party register is validated by the commissioning document. The asset register is reviewed against the register of exceptions. The remote access path is reviewed against the signed exception log. The classification scheme is measured against the signed exception log. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is measured against the most recent exercise record. The access review process is traced to the signed exception log. The backup rotation is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

7. Every internet-facing service

The change process is measured against the signed exception log. The metric set is reconciled with the dependency map. The monitoring pipeline is compared with the signed exception log. Any deviation requires written approval and an expiry date.

- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The endpoint baseline is compared with the ticket history for the period. The cloud baseline is evidenced by the dependency map. Each administrative account is reviewed against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is validated by the previous year's assessment. The encryption standard is reviewed against the approved design baseline. The threat model is evidenced by the most recent exercise record. The segmentation boundary is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

Every internet-facing service is validated by the register of exceptions. The endpoint baseline is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is reviewed against the previous year's assessment. The change process is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is reviewed against the evidence pack held by the owner. The retention schedule is evidenced by the agreed service level. Each administrative account is traced to the previous year's assessment. The backup rotation is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The metric set is measured against the register of exceptions. Every internet-facing service is compared with the most recent exercise record. The remote access path is compared with the commissioning document. The encryption standard is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is validated by the register of exceptions. The endpoint baseline is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

8. The remote access path

The vendor register is evidenced by the commissioning document. The identity lifecycle is traced to the previous year's assessment. The awareness cycle is traced to the dependency map. The identity lifecycle is reviewed against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is evidenced by the current written standard. The mobile standard is documented alongside the commissioning document. The patch calendar is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is reviewed against the approved design baseline. The awareness cycle is reviewed against the quarterly review notes. The retention schedule is evidenced by the ticket history for the period. The privileged access list is validated by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is traced to the register of exceptions. Every internet-facing service is validated by the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is evidenced by the dependency map. The privileged access list is compared with the evidence pack held by the owner. The email authentication record is validated by the quarterly review notes. The awareness cycle is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is validated by the dependency map. The identity lifecycle is measured against the signed exception log. The identity lifecycle is reviewed against the approved design baseline. The cloud baseline is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The vendor register is reviewed against the dependency map. The classification scheme is evidenced by the quarterly review notes. The asset register is evidenced by the previous year's assessment. The mobile standard is validated by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The change process is traced to the ticket history for the period. The third-party register is checked against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is traced to the register of exceptions. The vendor register is traced to the signed exception log. Testing covers the failure case, not only the happy path.

The privileged access list is traced to the commissioning document. The privileged access list is checked against the register of exceptions. The vulnerability queue is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The change process is checked against the previous year's assessment. The continuity plan is reviewed against the register of exceptions. The access review process is documented alongside the most recent exercise record. The encryption standard is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The segmentation boundary is checked against the approved design baseline. The monitoring pipeline is checked against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Test result attached to the record.
- Escalation path agreed with the service owner.

Every internet-facing service is reconciled with the previous year's assessment. The recovery test is evidenced by the agreed service level. The segmentation boundary is documented alongside the commissioning document. The third-party register is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The patch calendar is evidenced by the approved design baseline. The recovery test is documented alongside the register of exceptions. The cloud baseline is documented alongside the approved design baseline. Every internet-facing service is measured against the register of exceptions. Records are retained only as long as the schedule requires.

The encryption standard is checked against the evidence pack held by the owner. The cloud baseline is checked against the agreed service level. The identity lifecycle is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The cloud baseline is validated by the previous year's assessment. The segmentation boundary is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is checked against the agreed service level. The segmentation boundary is documented alongside the agreed service level. Each administrative account is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

9. The monitoring pipeline

The patch calendar is evidenced by the signed exception log. The risk register is reconciled with the ticket history for the period. Each administrative account is documented alongside the signed exception log. The email authentication record is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The backup rotation is validated by the previous year's assessment. The mobile standard is compared with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The mobile standard is reviewed against the register of exceptions. The physical controls is reviewed against the dependency map. The asset register is reviewed against the evidence pack held by the owner. The change process is reconciled with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is evidenced by the dependency map. The third-party register is checked against the dependency map. The change process is checked against the commissioning document. Each administrative account is traced to the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is checked against the ticket history for the period. The segmentation boundary is evidenced by the commissioning document. The physical controls is measured against the register of exceptions. The classification scheme is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The privileged access list is evidenced by the register of exceptions. The monitoring pipeline is evidenced by the approved design baseline. Third parties must demonstrate the control before access is granted.

The physical controls is reviewed against the ticket history for the period. The vendor register is validated by the quarterly review notes. The continuity plan is evidenced by the commissioning document. The intent is to make the safe path the default rather than an exception.

10. The patch calendar

The vulnerability queue is compared with the commissioning document. The continuity plan is documented alongside the dependency map. The hardened build is documented alongside the quarterly review notes. Metrics are reported as trends rather than single data points.

The risk register is compared with the quarterly review notes. The vulnerability queue is reconciled with the quarterly review notes. The change process is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

The third-party register is evidenced by the current written standard. The privileged access list is documented alongside the ticket history for the period. The backup rotation is reconciled with the agreed service level. Each administrative account is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is evidenced by the dependency map. The vendor register is compared with the commissioning document. The hardened build is reviewed against the commissioning document. The vulnerability queue is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is reviewed against the commissioning document. The cloud baseline is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is reconciled with the most recent exercise record. The physical controls is evidenced by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is reconciled with the ticket history for the period. The third-party register is compared with the agreed service level. The remote access path is checked against the current written standard. The remote access path is reviewed against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The mobile standard is traced to the ticket history for the period. The vulnerability queue is validated by the current written standard. The identity lifecycle is compared with the ticket history for the period. The mobile standard is traced to the ticket history for the period. Third parties must demonstrate the control before access is granted.

The physical controls is reconciled with the most recent exercise record. The vendor register is documented alongside the commissioning document. The endpoint baseline is checked against the dependency map. The identity lifecycle is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is checked against the ticket history for the period. The threat model is traced to the dependency map. The awareness cycle is documented alongside the most recent exercise record. The encryption standard is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is compared with the signed exception log. The threat model is reconciled with the ticket history for the period. Each administrative account is validated by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is reviewed against the evidence pack held by the owner. The cloud baseline is validated by the current written standard. The segmentation boundary is validated by the agreed service level. The patch calendar is checked against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The hardened build is reconciled with the previous year's assessment. The classification scheme is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is checked against the register of exceptions. The monitoring pipeline is compared with the dependency map. The control is tested at least once every twelve months.

The vulnerability queue is checked against the current written standard. The classification scheme is validated by the agreed service level. The identity lifecycle is reviewed against the ticket history for the period. The awareness cycle is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The change process is validated by the agreed service level. The threat model is measured against the register of exceptions. Each administrative account is reconciled with the dependency map. Every internet-facing service is reconciled with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is evidenced by the current written standard. The vulnerability queue is compared with the commissioning document. The physical controls is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The classification scheme is evidenced by the agreed service level. The access review process is reconciled with the register of exceptions. The mobile standard is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is documented alongside the most recent exercise record. The vendor register is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The encryption standard is checked against the quarterly review notes. The classification scheme is reviewed against the agreed service level. Third parties must demonstrate the control before access is granted.

The classification scheme is compared with the signed exception log. The remote access path is traced to the signed exception log. Any deviation requires written approval and an expiry date.

The vulnerability queue is reviewed against the quarterly review notes. The continuity plan is evidenced by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is measured against the ticket history for the period. The mobile standard is checked against the most recent exercise record. Each administrative account is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The vendor register is traced to the signed exception log. The identity lifecycle is reviewed against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is measured against the dependency map. The threat model is traced to the evidence pack held by the owner. The segmentation boundary is evidenced by the dependency map. The identity lifecycle is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The asset register is compared with the register of exceptions. The endpoint baseline is reviewed against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is documented alongside the approved design baseline. The cloud baseline is validated by the quarterly review notes. The vulnerability queue is checked against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The classification scheme is checked against the commissioning document. The recovery test is traced to the register of exceptions. The access review process is validated by the most recent exercise record. Every internet-facing service is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

11. The asset register

The threat model is traced to the current written standard. The change process is checked against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The hardened build is checked against the evidence pack held by the owner. The mobile standard is traced to the agreed service level. The continuity plan is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The threat model is evidenced by the signed exception log. The risk register is validated by the register of exceptions. The backup rotation is checked against the quarterly review notes. The segmentation boundary is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The recovery test is traced to the commissioning document. The patch calendar is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

The risk register is reconciled with the approved design baseline. Every internet-facing service is documented alongside the approved design baseline. The metric set is evidenced by the register of exceptions. The hardened build is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The vendor register is compared with the quarterly review notes. The mobile standard is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

12. The mobile standard

The encryption standard is reviewed against the register of exceptions. The email authentication record is documented alongside the ticket history for the period. The asset register is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

Each administrative account is compared with the signed exception log. The classification scheme is validated by the signed exception log. The backup rotation is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The access review process is traced to the register of exceptions. The hardened build is documented alongside the previous year's assessment. The identity lifecycle is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is reconciled with the most recent exercise record. The retention schedule is measured against the approved design baseline. The classification scheme is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

The access review process is compared with the approved design baseline. The privileged access list is reconciled with the dependency map. The patch calendar is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The access review process is reconciled with the commissioning document. The physical controls is reviewed against the agreed service level. The remote access path is reviewed against the agreed service level. The patch calendar is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The risk register is measured against the previous year's assessment. Each administrative account is reviewed against the commissioning document. Metrics are reported as trends rather than single data points.

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

The hardened build is reviewed against the quarterly review notes. The remote access path is compared with the signed exception log. The recovery test is traced to the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The third-party register is checked against the previous year's assessment. The threat model is reconciled with the current written standard. The patch calendar is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The continuity plan is measured against the dependency map. The asset register is traced to the signed exception log. The identity lifecycle is reviewed against the dependency map. The remote access path is measured against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is compared with the signed exception log. The vulnerability queue is measured against the register of exceptions. The email authentication record is evidenced by the most recent exercise record. The retention schedule is checked against the approved design baseline. Any deviation requires written approval and an expiry date.

- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Review date scheduled and visible.

The patch calendar is checked against the ticket history for the period. The remote access path is documented alongside the approved design baseline. The vendor register is reconciled with the agreed service level. The awareness cycle is evidenced by the dependency map. The control is tested at least once every twelve months.

The risk register is validated by the quarterly review notes. The segmentation boundary is compared with the previous year's assessment. Every internet-facing service is reviewed against the dependency map. The awareness cycle is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The retention schedule is documented alongside the quarterly review notes. The access review process is evidenced by the register of exceptions. The physical controls is checked against the agreed service level. The vendor register is validated by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is validated by the current written standard. The classification scheme is evidenced by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The risk register is reconciled with the previous year's assessment. The backup rotation is reconciled with the signed exception log. The continuity plan is reconciled with the commissioning document. Records are retained only as long as the schedule requires.

The third-party register is checked against the signed exception log. The retention schedule is reconciled with the ticket history for the period. The monitoring pipeline is traced to the dependency map. The retention schedule is validated by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is reconciled with the approved design baseline. The cloud baseline is checked against the signed exception log. The mobile standard is documented alongside the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is traced to the quarterly review notes. The risk register is reviewed against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The risk register is documented alongside the evidence pack held by the owner. The metric set is reconciled with the dependency map. The vendor register is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The vulnerability queue is validated by the most recent exercise record. The classification scheme is compared with the previous year's assessment. The change process is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is documented alongside the current written standard. The metric set is evidenced by the dependency map. The classification scheme is validated by the register of exceptions. The classification scheme is reconciled with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is validated by the most recent exercise record. The backup rotation is evidenced by the approved design baseline. The backup rotation is compared 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 change process is reconciled with the approved design baseline. The recovery test is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

14. The encryption standard

The classification scheme is checked against the most recent exercise record. The mobile standard is measured against the ticket history for the period. Every internet-facing service is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is reviewed against the most recent exercise record. Every internet-facing service is checked against the ticket history for the period. The remote access path is documented alongside the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the approved design baseline. The classification scheme is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The metric set is evidenced by the quarterly review notes. The recovery test is evidenced by the commissioning document. The access review process is validated by the most recent exercise record. The continuity plan is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reconciled with the most recent exercise record. The mobile standard is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is checked against the dependency map. The encryption standard is reviewed against the current written standard. Any deviation requires written approval and an expiry date.

The risk register is measured against the agreed service level. The change process is reviewed against the agreed service level. The access review process is traced to the quarterly review notes. The endpoint baseline is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The endpoint baseline is measured against the current written standard. The identity lifecycle is traced to the register of exceptions. The control is tested at least once every twelve months.

15. The third-party register

The email authentication record is documented alongside the evidence pack held by the owner. The change process is compared with the most recent exercise record. The control is tested at least once every twelve months.

The monitoring pipeline is reconciled with the signed exception log. The recovery test is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The threat model is reconciled with the approved design baseline. The threat model is evidenced by the most recent exercise record. The backup rotation is documented alongside the evidence pack held by the owner. The access review process is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is compared with the agreed service level. Each administrative account is measured against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The asset register is measured against the signed exception log. The vulnerability queue is traced to the commissioning document. The privileged access list is measured against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is traced to the commissioning document. The hardened build is compared with the signed exception log. The metric set is evidenced by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is validated by the approved design baseline. The continuity plan is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

The backup rotation is reconciled with the current written standard. The encryption standard is measured against the commissioning document. The cloud baseline is validated by the commissioning document. The encryption standard is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The physical controls is traced to the signed exception log. The physical controls is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

16. The awareness cycle

The vendor register is checked against the previous year's assessment. The patch calendar is documented alongside the evidence pack held by the owner. The remote access path is checked against the current written standard. The control is tested at least once every twelve months.

The physical controls is reviewed against the most recent exercise record. The threat model is documented alongside the previous year's assessment. Every internet-facing service is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

17. The privileged access list

The threat model is evidenced by the ticket history for the period. The email authentication record is reviewed against the current written standard. The metric set is reviewed against the approved design baseline. The privileged access list is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

The email authentication record is validated by the register of exceptions. The patch calendar is checked against the ticket history for the period. The asset register is reviewed against the ticket history for the period. The backup rotation is reviewed against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The asset register is traced to the current written standard. The mobile standard is measured against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The vendor register is reconciled with the approved design baseline. The cloud baseline is compared with the register of exceptions. The cloud baseline is evidenced by the signed exception log. The privileged access list is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is reconciled with the agreed service level. The email authentication record is reviewed against the quarterly review notes. The encryption standard is reconciled with the agreed service level. The awareness cycle is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The classification scheme is compared with the approved design baseline. The access review process is measured against the register of exceptions. The asset register is compared with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

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

The recovery test is evidenced by the quarterly review notes. The awareness cycle is compared with the most recent exercise record. The segmentation boundary is evidenced by the current written standard. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is documented alongside the agreed service level. The cloud baseline is reviewed against the agreed service level. The remote access path is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

The monitoring pipeline is documented alongside the quarterly review notes. The physical controls is documented alongside the register of exceptions. The backup rotation is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is traced to the ticket history for the period. The identity lifecycle is compared with the previous year's assessment. The metric set is checked against the agreed service level. The mobile standard is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is reconciled with the quarterly review notes. The metric set is compared with the approved design baseline. The control is tested at least once every twelve months.

The patch calendar is traced to the commissioning document. The remote access path is measured against the ticket history for the period. The remote access path is validated by the quarterly review notes. The retention schedule is compared with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is traced to the previous year's assessment. The segmentation boundary is evidenced by the evidence pack held by the owner. The vendor register is reviewed against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is reconciled with the most recent exercise record. The cloud baseline is checked against the quarterly review notes. The patch calendar is reconciled with the quarterly review notes. The segmentation boundary is checked against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is measured against the agreed service level. The threat model is reconciled with the quarterly review notes. The physical controls is compared with the dependency map. The third-party register is checked against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is measured against the current written standard. The email authentication record is traced to the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

18. The privileged access list

The change process is compared with the evidence pack held by the owner. The hardened build is reviewed against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The change process is measured against the commissioning document. The remote access path is validated by the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The metric set is evidenced by the signed exception log. The mobile standard is compared with the ticket history for the period. The endpoint baseline is reconciled with the ticket history for the period. The endpoint baseline is compared with the ticket history for the period. The control is tested at least once every twelve months.

The cloud baseline is evidenced by the current written standard. The hardened build is evidenced by the evidence pack held by the owner. The cloud baseline is validated by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is traced to the agreed service level. The monitoring pipeline is evidenced by the most recent exercise record. The access review process is compared with the register of exceptions. The third-party register is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is evidenced by the commissioning document. Every internet-facing service is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

19. The monitoring pipeline

The backup rotation is reconciled with the register of exceptions. The monitoring pipeline is validated by the evidence pack held by the owner. The patch calendar is measured against the evidence pack held by the owner. The endpoint baseline is traced to the ticket history for the period. Metrics are reported as trends rather than single data points.

The mobile standard is measured against the register of exceptions. The vulnerability queue is reconciled with the most recent exercise record. The classification scheme is validated by the previous year's assessment. The segmentation boundary is traced to the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The vendor register is compared with the register of exceptions. The awareness cycle is reviewed against the most recent exercise record. The vulnerability queue is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

The privileged access list is reviewed against the ticket history for the period. The mobile standard is measured against the current written standard. The cloud baseline is measured against the approved design baseline. The identity lifecycle is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.

20. The mobile standard

- Acceptance criteria written before work starts.
- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.

Each administrative account is traced to the register of exceptions. The monitoring pipeline is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is checked against the previous year's assessment. The segmentation boundary is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is compared with the signed exception log. The physical controls is validated by the previous year's assessment. The encryption standard is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The risk register is measured against the dependency map. Each administrative account is traced to the most recent exercise record. The change process is traced to the evidence pack held by the owner. Every internet-facing service is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is traced to the evidence pack held by the owner. The remote access path is measured against the dependency map. The third-party register is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The continuity plan is compared with the most recent exercise record. The third-party register is measured against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is documented alongside the previous year's assessment. The hardened build is measured against the dependency map. The recovery test is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The risk register is reviewed against the quarterly review notes. The encryption standard is reviewed against the ticket history for the period. The change process is validated by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

21. The asset register

The retention schedule is reviewed against the current written standard. The backup rotation is documented alongside the current written standard. Evidence is kept for audit, insurance and regulator requests.

The asset register is reconciled with the signed exception log. The email authentication record is checked against the current written standard. The vendor register is validated by the signed exception log. The encryption standard is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is documented alongside the previous year's assessment. The awareness cycle is measured against the signed exception log. The identity lifecycle is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

The recovery test is checked against the ticket history for the period. The segmentation boundary is compared with the evidence pack held by the owner. The encryption standard is checked against the signed exception log. The third-party register is documented alongside the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is compared with the dependency map. The endpoint baseline is reviewed against the previous year's assessment. The backup rotation is compared with the agreed service level. The intent is to make the safe path the default rather than an exception.

The awareness cycle is checked against the agreed service level. The retention schedule is evidenced by the evidence pack held by the owner. The remote access path is evidenced by the agreed service level. The vulnerability queue is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The vendor register is evidenced by the current written standard. The cloud baseline is traced to the most recent exercise record. The awareness cycle is traced to the dependency map. The vendor register is measured against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The change process is evidenced by the agreed service level. The hardened build is checked against the previous year's assessment. The risk register is measured against the quarterly review notes. The identity lifecycle is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The physical controls is traced to the quarterly review notes. The vulnerability queue is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.