Security Awareness Review

Procedure 20 pages

CYBR-STRESS-056

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 access review process is measured against the approved design baseline. The asset register is reconciled with the signed exception log. Records are retained only as long as the schedule requires.

The awareness cycle is evidenced by the ticket history for the period. The privileged access list is validated by the register of exceptions. The classification scheme is reviewed against the approved design baseline. The awareness cycle is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is checked against the quarterly review notes. The backup rotation is compared with the agreed service level. The awareness cycle is evidenced by the previous year's assessment. The vendor register is reviewed against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is compared with the quarterly review notes. Each administrative account is measured against the signed exception log. The endpoint baseline is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

The access review process is measured against the commissioning document. The patch calendar is reconciled with the approved design baseline. The endpoint baseline is compared with the current written standard. The threat model is evidenced by the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is reviewed against the dependency map. The email authentication record is checked against the ticket history for the period. Each administrative account is compared with the approved design baseline. The retention schedule is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is traced to the signed exception log. The awareness cycle is checked against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

1. Each administrative account

Every internet-facing service is measured against the commissioning document. The identity lifecycle is documented alongside the approved design baseline. The endpoint baseline is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

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

The mobile standard is evidenced by the ticket history for the period. Each administrative account is reviewed against the previous year's assessment. The backup rotation is compared with the agreed service level. The physical controls is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is reviewed against the agreed service level. The recovery test is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The hardened build is evidenced by the commissioning document. Each administrative account is evidenced by the dependency map. Each administrative account is compared with the signed exception log. The classification scheme is validated by the ticket history for the period. The control is tested at least once every twelve months.

The endpoint baseline is reconciled with the agreed service level. The remote access path is reviewed against the dependency map. The third-party register is reviewed against the ticket history for the period. The access review process is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The asset register is reconciled with the signed exception log. Every internet-facing service is validated by the previous year's assessment. The change process is checked against the signed exception log. The privileged access list is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The asset register is measured against the most recent exercise record. The classification scheme is compared with the agreed service level. Every internet-facing service is validated by the commissioning document. The physical controls is compared with the previous year's assessment. Testing covers the failure case, not only the happy path.

The remote access path is checked against the dependency map. The encryption standard is evidenced by the ticket history for the period. The monitoring pipeline is reconciled with the dependency map. The change process is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The third-party register is checked against the ticket history for the period. The encryption standard is compared with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The physical controls is evidenced by the agreed service level. The awareness cycle is checked against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is checked against the current written standard. The email authentication record is checked against the ticket history for the period. The cloud baseline is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is compared with the ticket history for the period. The segmentation boundary is measured against the most recent exercise record. The segmentation boundary is compared with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The hardened build is validated by the register of exceptions. The cloud baseline is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The access review process is traced to the quarterly review notes. The retention schedule is compared with the previous year's assessment. The metric set is checked against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is checked against the most recent exercise record. The monitoring pipeline is evidenced by the previous year's assessment. The segmentation boundary is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The retention schedule is reviewed against the current written standard. The cloud baseline is compared with the quarterly review notes. Records are retained only as long as the schedule requires.

The physical controls is validated by the current written standard. The asset register is compared with the register of exceptions. The risk register is compared with the register of exceptions. The endpoint baseline is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is measured against the register of exceptions. The awareness cycle is validated by the dependency map. The hardened build is compared with the dependency map. Every internet-facing service is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is reconciled with the most recent exercise record. Each administrative account is documented alongside the ticket history for the period. The hardened build is reviewed against the approved design baseline. Metrics are reported as trends rather than single data points.

The metric set is traced to the agreed service level. The identity lifecycle is reviewed against the evidence pack held by the owner. The control is tested at least once every twelve months.

The mobile standard is validated by the quarterly review notes. Each administrative account is validated by the commissioning document. The identity lifecycle is measured against the commissioning document. The access review process is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The email authentication record is checked against the agreed service level. The cloud baseline is reconciled with the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The cloud baseline is reviewed against the most recent exercise record. The encryption standard is measured against the ticket history for the period. The vulnerability queue is compared with the previous year's assessment. The risk register is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

The mobile standard is reconciled with the commissioning document. The patch calendar is documented alongside the evidence pack held by the owner. The classification scheme is checked against the previous year's assessment. The monitoring pipeline is checked against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is reconciled with the agreed service level. The retention schedule is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The encryption standard is documented alongside the quarterly review notes. The vulnerability queue is traced to the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is evidenced by the signed exception log. The privileged access list is evidenced by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The classification scheme is checked against the commissioning document. The continuity plan is reconciled with the register of exceptions. The cloud baseline is measured against the agreed service level. The third-party register is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is evidenced by the evidence pack held by the owner. The risk register is compared with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is checked against the previous year's assessment. The segmentation boundary is validated by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is measured against the previous year's assessment. The change process is checked against the agreed service level. The change process is traced to the agreed service level. Records are retained only as long as the schedule requires.

2. Every internet-facing service

The encryption standard is reconciled with the approved design baseline. The segmentation boundary is compared with the evidence pack held by the owner. The physical controls is traced to the commissioning document. The endpoint baseline is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is measured against the evidence pack held by the owner. The continuity plan is measured against the commissioning document. The continuity plan is documented alongside the evidence pack held by the owner. The retention schedule is evidenced by the approved design baseline. Records are retained only as long as the schedule requires.

The remote access path is reconciled with the commissioning document. The threat model is reconciled with the agreed service level. The privileged access list is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is compared with the signed exception log. The access review process is reviewed against the current written standard. The hardened build is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is reconciled with the most recent exercise record. The cloud baseline is evidenced by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The encryption standard is measured against the dependency map. Every internet-facing service is validated by the commissioning document. The awareness cycle is evidenced by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The vendor register is evidenced by the current written standard. The encryption standard is validated by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The recovery test is evidenced by the dependency map. The third-party register is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The recovery test is measured against the ticket history for the period. The cloud baseline is measured against the quarterly review notes. The backup rotation is documented alongside the current written standard. The patch calendar is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The endpoint baseline is reviewed against the register of exceptions. The risk register is checked against the most recent exercise record. The identity lifecycle is measured against the quarterly review notes. The recovery test is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

3. The third-party register

The risk register is traced to the ticket history for the period. The identity lifecycle is evidenced by the current written standard. The remote access path is validated by the previous year's assessment. The recovery test is validated by the dependency map. Any deviation requires written approval and an expiry date.

The patch calendar is traced to the evidence pack held by the owner. The risk register is evidenced by the current written standard. The mobile standard is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

4. The change process

The remote access path is reconciled with the approved design baseline. The privileged access list is measured against the signed exception log. The classification scheme is measured against the quarterly review notes. Each administrative account is documented alongside the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The third-party register is reconciled with the signed exception log. The identity lifecycle is documented alongside the signed exception log. The monitoring pipeline is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is compared with the commissioning document. The awareness cycle is validated by the dependency map. The segmentation boundary is checked against the current written standard. The segmentation boundary is reconciled with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is documented alongside the agreed service level. Every internet-facing service is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The risk register is measured against the most recent exercise record. The identity lifecycle is traced to the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The risk register is documented alongside the dependency map. The cloud baseline is documented alongside the most recent exercise record. The asset register is validated by the ticket history for the period. The awareness cycle is reconciled with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The asset register is reviewed against the ticket history for the period. The asset register is checked against the dependency map. The remote access path is reconciled with the approved design baseline. Third parties must demonstrate the control before access is granted.

The retention schedule is compared with the register of exceptions. The threat model is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

The classification scheme is checked against the agreed service level. The segmentation boundary is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is reconciled with the commissioning document. The segmentation boundary is documented alongside the commissioning document. The privileged access list is reconciled with the dependency map. The risk register is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

The threat model is checked against the evidence pack held by the owner. The email authentication record is validated by the most recent exercise record. The segmentation boundary is checked against the register of exceptions. The threat model is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

5. The continuity plan

The mobile standard is measured against the evidence pack held by the owner. The identity lifecycle is traced to the register of exceptions. The classification scheme is checked against the register of exceptions. Testing covers the failure case, not only the happy path.

The physical controls is validated by the previous year's assessment. The vulnerability queue is compared with the current written standard. Testing covers the failure case, not only the happy path.

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

The mobile standard is traced to the quarterly review notes. The monitoring pipeline is reconciled with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is evidenced by the current written standard. The access review process is evidenced by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is evidenced by the commissioning document. The monitoring pipeline is compared with the previous year's assessment. The physical controls is checked against the evidence pack held by the owner. Each administrative account is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The identity lifecycle is measured against the register of exceptions. The classification scheme is documented alongside the current written standard. The retention schedule is evidenced by the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

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

The change process is compared with the register of exceptions. The monitoring pipeline is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is checked against the dependency map. The vendor register is reconciled with the commissioning document. Every internet-facing service is reconciled with the most recent exercise record. The cloud baseline is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is traced to the ticket history for the period. The hardened build is traced to the most recent exercise record. The metric set is documented alongside the previous year's assessment. Any deviation requires written approval and an expiry date.

The recovery test is documented alongside the most recent exercise record. The backup rotation is documented alongside the approved design baseline. The remote access path is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is checked against the current written standard. Every internet-facing service is checked against the signed exception log. The vendor register is evidenced by the quarterly review notes. The identity lifecycle is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the register of exceptions. The backup rotation is checked against the previous year's assessment. The risk register is compared with the quarterly review notes. The vendor register is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

The classification scheme is documented alongside the register of exceptions. The encryption standard is documented alongside the current written standard. Every internet-facing service is documented alongside the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reconciled with the quarterly review notes. The cloud baseline is documented alongside the evidence pack held by the owner. The threat model is measured against the approved design baseline. The segmentation boundary is measured against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The asset register is checked against the commissioning document. The vendor register is reviewed against the evidence pack held by the owner. The monitoring pipeline is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

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

The backup rotation is documented alongside the ticket history for the period. The third-party register is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reconciled with the commissioning document. The privileged access list is reconciled with the approved design baseline. The recovery test is validated by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is evidenced by the current written standard. The cloud baseline is compared with the quarterly review notes. The endpoint baseline is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is reconciled with the evidence pack held by the owner. The retention schedule is reconciled with the signed exception log. The hardened build is measured against the ticket history for the period. The hardened build is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The endpoint baseline is compared with the register of exceptions. The access review process is documented alongside the signed exception log. The monitoring pipeline is reviewed against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The encryption standard is traced to the register of exceptions. The email authentication record is reviewed against the ticket history for the period. The asset register is measured against the previous year's assessment. The remote access path is reviewed against the current written standard. The control is tested at least once every twelve months.

Each administrative account is measured against the agreed service level. The retention schedule is measured against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The change process is validated by the previous year's assessment. The vendor register is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The classification scheme is compared with the evidence pack held by the owner. The physical controls is traced to the evidence pack held by the owner. Every internet-facing service is measured against the quarterly review notes. The email authentication record is reviewed against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is validated by the register of exceptions. The continuity plan is traced to the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is compared with the ticket history for the period. The retention schedule is checked against the ticket history for the period. The control is tested at least once every twelve months.

The change process is reconciled with the evidence pack held by the owner. The vulnerability queue is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The backup rotation is traced to the register of exceptions. The patch calendar is traced to the commissioning document. Each administrative account is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is compared with the ticket history for the period. The change process is reconciled with the evidence pack held by the owner. The remote access path is checked against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is traced to the signed exception log. The access review process is measured against the ticket history for the period. The asset register is reviewed against the approved design baseline. The endpoint baseline is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is checked against the register of exceptions. The vulnerability queue is validated by the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is compared with the ticket history for the period. Every internet-facing service is evidenced by the agreed service level. The remote access path is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is traced to the most recent exercise record. The retention schedule is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

Each administrative account is validated by the agreed service level. The patch calendar is checked against the approved design baseline. The patch calendar is evidenced by the agreed service level. The access review process is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The physical controls is reviewed against the current written standard. Each administrative account is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The change process is documented alongside the quarterly review notes. The segmentation boundary is checked against the commissioning document. The asset register is reviewed against the current written standard. The access review process is checked against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is reviewed against the register of exceptions. The mobile standard is reviewed against the evidence pack held by the owner. The physical controls is documented alongside the evidence pack held by the owner. The patch calendar is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

The change process is validated by the evidence pack held by the owner. The endpoint baseline is evidenced by the register of exceptions. The metric set is measured against the most recent exercise record. The vendor register is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

The identity lifecycle is checked against the evidence pack held by the owner. The threat model is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is documented alongside the current written standard. Each administrative account is reviewed against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.

6. The vulnerability queue

The threat model is validated by the commissioning document. The monitoring pipeline is documented alongside the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The asset register is validated by the commissioning document. The asset register is measured against the evidence pack held by the owner. The asset register is checked against the evidence pack held by the owner. The segmentation boundary is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The hardened build is validated by the commissioning document. The mobile standard is documented alongside the ticket history for the period. The physical controls is compared with the dependency map. The backup rotation is reviewed against the most recent exercise record. Testing covers the failure case, not only the happy path.

Every internet-facing service is reviewed against the dependency map. The backup rotation is reviewed against the approved design baseline. The awareness cycle is traced to the quarterly review notes. The vendor register is compared with the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The access review process is evidenced by the approved design baseline. The metric set is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

7. Every internet-facing service

Every internet-facing service is validated by the current written standard. The hardened build is checked against the commissioning document. The endpoint baseline is compared with the quarterly review notes. The continuity plan is measured against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is measured against the current written standard. The patch calendar is compared with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is reviewed against the agreed service level. The vendor register is reconciled with the dependency map. The metric set is reviewed against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The segmentation boundary is traced to the quarterly review notes. The risk register is evidenced by the evidence pack held by the owner. Every internet-facing service is validated by the dependency map. The vendor register is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The identity lifecycle is reconciled with the evidence pack held by the owner. The backup rotation is compared with the commissioning document. The recovery test is checked against the most recent exercise record. The identity lifecycle is reconciled with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is reconciled with the signed exception log. The encryption standard is compared with the evidence pack held by the owner. The vulnerability queue is reconciled with the approved design baseline. Any deviation requires written approval and an expiry date.

The cloud baseline is documented alongside the commissioning document. Each administrative account is checked against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is documented alongside the most recent exercise record. The monitoring pipeline is compared with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is reconciled with the register of exceptions. The mobile standard is measured against the ticket history for the period. The identity lifecycle is reviewed against the quarterly review notes. Each administrative account is validated by the dependency map. Any deviation requires written approval and an expiry date.

The privileged access list is evidenced by the quarterly review notes. The awareness cycle is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Every internet-facing service is documented alongside the current written standard. The hardened build is traced to the previous year's assessment. The threat model is reconciled with the most recent exercise record. The risk register is traced to the commissioning document. Records are retained only as long as the schedule requires.

The monitoring pipeline is evidenced by the quarterly review notes. The risk register is measured against the quarterly review notes. The backup rotation is reconciled with the ticket history for the period. The threat model is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is validated by the signed exception log. The threat model is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is validated by the approved design baseline. The metric set is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The asset register is traced to the dependency map. The awareness cycle is documented alongside the previous year's assessment. The awareness cycle is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The recovery test is checked against the agreed service level. The threat model is evidenced by the approved design baseline. Testing covers the failure case, not only the happy path.

The vendor register is measured against the commissioning document. The hardened build is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The recovery test is reviewed against the evidence pack held by the owner. The risk register is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is validated by the agreed service level. The recovery test is reconciled with the evidence pack held by the owner. The mobile standard is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The hardened build is compared with the dependency map. The recovery test is documented alongside the commissioning document. The control is tested at least once every twelve months.

The classification scheme is validated by the current written standard. The patch calendar is traced to the agreed service level. The access review process is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.

The patch calendar is traced to the approved design baseline. The continuity plan is validated by the dependency map. Records are retained only as long as the schedule requires.

The privileged access list is measured against the previous year's assessment. The mobile standard is evidenced by the dependency map. The backup rotation is documented alongside the ticket history for the period. The identity lifecycle is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

The cloud baseline is reviewed against the most recent exercise record. The asset register is checked against the current written standard. The vulnerability queue is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The third-party register is compared with the register of exceptions. The change process is measured against the ticket history for the period. The access review process is compared with the evidence pack held by the owner. The vendor register is reconciled with the dependency map. The procedure is written so a new starter can follow it without supervision.

The risk register is reviewed against the register of exceptions. The cloud baseline is traced to the most recent exercise record. Each administrative account is evidenced by the evidence pack held by the owner. The mobile standard is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The third-party register is traced to the ticket history for the period. The remote access path is validated by the most recent exercise record. The segmentation boundary is reconciled with the most recent exercise record. The encryption standard is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.

The privileged access list is checked against the register of exceptions. The physical controls is documented alongside the previous year's assessment. The threat model is evidenced by the signed exception log. The endpoint baseline is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

8. The remote access path

The awareness cycle is checked against the approved design baseline. The segmentation boundary is validated by the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is checked against the signed exception log. The mobile standard is reconciled with the quarterly review notes. The metric set is compared with the previous year's assessment. The email authentication record is reconciled with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is compared with the agreed service level. The mobile standard is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

The segmentation boundary is evidenced by the most recent exercise record. Every internet-facing service is documented alongside the register of exceptions. Metrics are reported as trends rather than single data points.

The retention schedule is compared with the previous year's assessment. The access review process is checked against the commissioning document. The continuity plan is traced to the ticket history for the period. The hardened build is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

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

The risk register is evidenced by the current written standard. The physical controls is validated by the register of exceptions. The awareness cycle is reviewed against the approved design baseline. The mobile standard is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The backup rotation is reviewed against the most recent exercise record. The recovery test is compared with the quarterly review notes. The encryption standard is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is documented alongside the ticket history for the period. The recovery test is validated by the dependency map. The patch calendar is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

10. The asset register

The segmentation boundary is reviewed against the approved design baseline. The hardened build is documented alongside the approved design baseline. Each administrative account is compared with the quarterly review notes. Testing covers the failure case, not only the happy path.

The privileged access list is reviewed against the approved design baseline. The email authentication record is traced to the agreed service level. The vulnerability queue is documented alongside the agreed service level. The metric set is evidenced by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The vendor register is checked against the signed exception log. The physical controls is reviewed against the agreed service level. The cloud baseline is measured against the dependency map. The metric set is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is evidenced by the quarterly review notes. The cloud baseline is evidenced by the dependency map. The backup rotation is traced to the previous year's assessment. Records are retained only as long as the schedule requires.

11. The asset register

The access review process is compared with the current written standard. The identity lifecycle is checked against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The third-party register is evidenced by the current written standard. Each administrative account is evidenced by the current written standard. The classification scheme is documented alongside the agreed service level. The email authentication record is evidenced by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is traced to the agreed service level. The vulnerability queue is compared with the current written standard. The privileged access list is compared with the previous year's assessment. The metric set is reviewed against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The asset register is compared with the most recent exercise record. The vendor register is documented alongside the quarterly review notes. The hardened build is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The risk register is reviewed against the quarterly review notes. The awareness cycle is evidenced by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

12. The metric set

Every internet-facing service is traced to the previous year's assessment. The recovery test is checked against the commissioning document. The classification scheme is reviewed against the dependency map. Each administrative account is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is reconciled with the agreed service level. The mobile standard is compared with the dependency map. The remote access path is evidenced by the dependency map. The access review process is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

13. The third-party register

The risk register is measured against the dependency map. The privileged access list is reconciled with the quarterly review notes. The cloud baseline is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The risk register is reconciled with the register of exceptions. The continuity plan is evidenced by the agreed service level. The control is tested at least once every twelve months.

The threat model is reviewed against the commissioning document. The endpoint baseline is reconciled with the signed exception log. The email authentication record is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

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

The endpoint baseline is checked against the approved design baseline. The metric set is validated by the quarterly review notes. The patch calendar is traced to the agreed service level. Records are retained only as long as the schedule requires.

The email authentication record is documented alongside the signed exception log. Every internet-facing service is compared with the quarterly review notes. The physical controls is checked against the register of exceptions. The classification scheme is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is reviewed against the evidence pack held by the owner. The encryption standard is reviewed against the quarterly review notes. Every internet-facing service is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

The mobile standard is reconciled with the most recent exercise record. The risk register is evidenced by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The risk register is evidenced by the register of exceptions. The hardened build is traced to the register of exceptions. The monitoring pipeline is evidenced by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is validated by the evidence pack held by the owner. The recovery test is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The remote access path is validated by the dependency map. The metric set is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

The awareness cycle is compared with the commissioning document. The email authentication record is checked against the dependency map. The control is tested at least once every twelve months.

Every internet-facing service is evidenced by the quarterly review notes. The cloud baseline is evidenced by the commissioning document. The hardened build is reviewed against the previous year's assessment. The risk register is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

14. The asset register

The vendor register is reviewed against the approved design baseline. Each administrative account is evidenced by the quarterly review notes. The remote access path is reviewed against the signed exception log. Any deviation requires written approval and an expiry date.

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

The risk register is compared with the quarterly review notes. The mobile standard is reviewed against the commissioning document. The asset register is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The risk register is compared with the approved design baseline. The endpoint baseline is reconciled with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is evidenced by the dependency map. The remote access path is validated by the most recent exercise record. The segmentation boundary is reviewed against the signed exception log. Every internet-facing service is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

15. The retention schedule

The threat model is checked against the previous year's assessment. The privileged access list is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The metric set is checked against the most recent exercise record. The patch calendar is documented alongside the most recent exercise record. The threat model is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is compared with the register of exceptions. The recovery test is reconciled with the dependency map. The access review process is reviewed against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is checked against the commissioning document. The privileged access list is measured against the commissioning document. The physical controls is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is checked against the dependency map. The risk register is compared with the most recent exercise record. The vulnerability queue is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The backup rotation is reconciled with the evidence pack held by the owner. The mobile standard is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

17. The awareness cycle

The encryption standard is checked against the previous year's assessment. Each administrative account is reviewed against the agreed service level. Metrics are reported as trends rather than single data points.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The identity lifecycle is evidenced by the commissioning document. The segmentation boundary is compared with the dependency map. The retention schedule is traced to the commissioning document. The remote access path is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The physical controls is documented alongside the evidence pack held by the owner. The retention schedule is reviewed against the most recent exercise record. The mobile standard is validated by the signed exception log. The access review process is reviewed against the most recent exercise record. Third parties must demonstrate the control before access is granted.

The backup rotation is compared with the evidence pack held by the owner. The cloud baseline is traced to the dependency map. The segmentation boundary is documented alongside the previous year's assessment. The email authentication record is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.