STRESS TEST DOCUMENT

Network Segmentation Review

Exercise record 15 pages

CYBR-STRESS-059

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 register of exceptions. The recovery test is compared with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The remote access path is validated by the quarterly review notes. The privileged access list is measured against the signed exception log. The monitoring pipeline is validated by the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The hardened build is evidenced by the dependency map. The change process is validated by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is compared with the evidence pack held by the owner. The encryption standard is reviewed against the ticket history for the period. The continuity plan is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is validated by the previous year's assessment. The metric set is checked against the register of exceptions. Metrics are reported as trends rather than single data points.

The encryption standard is reviewed against the ticket history for the period. The risk register is checked against the agreed service level. The segmentation boundary is checked against the dependency map. Records are retained only as long as the schedule requires.

Every internet-facing service is evidenced by the commissioning document. The retention schedule is measured against the most recent exercise record. The patch calendar is reviewed against the signed exception log. Any deviation requires written approval and an expiry date.

The backup rotation is reviewed against the agreed service level. The classification scheme is documented alongside the quarterly review notes. The metric set is reconciled with the signed exception log. The awareness cycle 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 measured against the most recent exercise record. The classification scheme is reviewed against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is checked against the approved design baseline. The threat model is reconciled with the dependency map. The change process is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is evidenced by the dependency map. The change process is validated by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The remote access path is measured against the previous year's assessment. The retention schedule is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the quarterly review notes. The physical controls is reviewed against the evidence pack held by the owner. Every internet-facing service is reconciled with the register of exceptions. Every internet-facing service is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is compared with the most recent exercise record. The vulnerability queue is reconciled with the signed exception log. Third parties must demonstrate the control before access is granted.

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

Every internet-facing service is validated by the commissioning document. The email authentication record is compared with the signed exception log. The backup rotation is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

The asset register is reviewed against the most recent exercise record. The identity lifecycle is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The metric set is reviewed against the dependency map. The identity lifecycle is traced to the approved design baseline. The third-party register is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reviewed against the signed exception log. The backup rotation is measured against the signed exception log. The hardened build is measured against the dependency map. The metric set is measured against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The threat model is measured against the approved design baseline. The risk register is validated by the quarterly review notes. The mobile standard is traced to the agreed service level. The cloud baseline is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

1. The patch calendar

The monitoring pipeline is traced to the agreed service level. The encryption standard is documented alongside the dependency map. The retention schedule is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The change process is compared with the agreed service level. The classification scheme is measured against the ticket history for the period. The segmentation boundary is checked against the commissioning document. The change process is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The recovery test is measured against the most recent exercise record. The identity lifecycle is evidenced by the approved design baseline. The privileged access list is traced to the previous year's assessment. The retention schedule is reconciled with the quarterly review notes. Metrics are reported as trends rather than single data points.

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

The metric set is traced to the register of exceptions. The identity lifecycle is traced to the dependency map. Metrics are reported as trends rather than single data points.

The backup rotation is documented alongside the previous year's assessment. The email authentication record is reviewed against the commissioning document. The email authentication record is measured against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The risk register is documented alongside the quarterly review notes. The vulnerability queue is checked against the most recent exercise record. The asset register is evidenced by the most recent exercise record. The awareness cycle is validated by the dependency map. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is documented alongside the current written standard. The remote access path is reviewed against the signed exception log. The monitoring pipeline is validated by the commissioning document. Any deviation requires written approval and an expiry date.

The encryption standard is measured against the dependency map. Every internet-facing service is measured against the quarterly review notes. The hardened build is documented alongside the approved design baseline. The recovery test is compared with the commissioning document. Metrics are reported as trends rather than single data points.

The recovery test is documented alongside the signed exception log. The remote access path is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

The cloud baseline is documented alongside the agreed service level. The metric set is checked against the ticket history for the period. Testing covers the failure case, not only the happy path.

The retention schedule is checked against the dependency map. The awareness cycle is compared with the current written standard. The third-party register is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is measured against the commissioning document. The change process is compared with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The change process is compared with the quarterly review notes. The access review process is compared with the register of exceptions. The backup rotation is compared with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The asset register is compared with the current written standard. Every internet-facing service is checked against the quarterly review notes. The recovery test is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The vendor register is checked against the most recent exercise record. The privileged access list is documented alongside the dependency map. The segmentation boundary is reviewed against the ticket history for the period. The vulnerability queue is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is traced to the agreed service level. The privileged access list is checked against the quarterly review notes. The asset register is compared with the current written standard. Testing covers the failure case, not only the happy path.

The access review process is traced to the commissioning document. The patch calendar is traced to the current written standard. Testing covers the failure case, not only the happy path.

The encryption standard is checked against the signed exception log. The retention schedule is checked against the commissioning document. The vendor register is documented alongside the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

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

The awareness cycle is reconciled with the most recent exercise record. The mobile standard is documented alongside the ticket history for the period. The retention schedule is evidenced by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is measured against the dependency map. The awareness cycle is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is reconciled with the most recent exercise record. The retention schedule is measured against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The cloud baseline is measured against the current written standard. The segmentation boundary is documented alongside the ticket history for the period. The control is tested at least once every twelve months.

The vendor register is traced to the dependency map. The metric set is evidenced by the dependency map. The vendor register is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is compared with the previous year's assessment. The threat model is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The risk register is documented alongside the signed exception log. The recovery test is documented alongside the commissioning document. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is measured against the approved design baseline. Every internet-facing service is checked against the approved design baseline. The identity lifecycle is measured against the commissioning document. The hardened build is compared with the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is documented alongside the agreed service level. The cloud baseline is traced to the most recent exercise record. The hardened build is measured against the approved design baseline. The privileged access list is documented alongside the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The hardened build is validated by the current written standard. The vulnerability queue is documented alongside the current written standard. Third parties must demonstrate the control before access is granted.

The third-party register is evidenced by the evidence pack held by the owner. The classification scheme is validated by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The asset register is compared with the previous year's assessment. The awareness cycle is checked against the evidence pack held by the owner. The patch calendar is documented alongside the commissioning document. The recovery test is documented alongside the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The recovery test is measured against the dependency map. The awareness cycle is validated by the agreed service level. The mobile standard is reconciled with the evidence pack held by the owner. The metric set is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

The email authentication record is evidenced by the most recent exercise record. The continuity plan is validated by the quarterly review notes. The classification scheme is measured against the most recent exercise record. The recovery test is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The vulnerability queue is validated by the agreed service level. The third-party register is compared with the evidence pack held by the owner. The risk register is reconciled with the approved design baseline. Third parties must demonstrate the control before access is granted.

The asset register is documented alongside the commissioning document. The vendor register is traced to the approved design baseline. The vulnerability queue is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

3. The email authentication record

The threat model is measured against the commissioning document. Each administrative account is measured against the dependency map. The privileged access list is checked against the current written standard. Third parties must demonstrate the control before access is granted.

The asset register is evidenced by the agreed service level. The remote access path is measured against the current written standard. The monitoring pipeline is reconciled with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The third-party register is validated by the approved design baseline. The retention schedule is traced to the most recent exercise record. The vulnerability queue is validated by the agreed service level. Records are retained only as long as the schedule requires.

The mobile standard is documented alongside the ticket history for the period. The monitoring pipeline is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reviewed against the previous year's assessment. The privileged access list is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

The cloud baseline is traced to the current written standard. The hardened build is traced to the signed exception log. The risk register is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is documented alongside the commissioning document. The third-party register is measured against the signed exception log. The privileged access list is compared with the previous year's assessment. The endpoint baseline is documented alongside the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is reviewed against the commissioning document. The risk register is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is measured against the signed exception log. The awareness cycle is measured against the most recent exercise record. The vulnerability queue is evidenced by the approved design baseline. The remote access path is checked against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reviewed against the signed exception log. The remote access path is checked against the commissioning document. The asset register is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is measured against the ticket history for the period. The backup rotation is evidenced by the commissioning document. The risk register is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The vendor register is measured against the register of exceptions. The monitoring pipeline is compared with the current written standard. The asset register is documented alongside the current written standard. The awareness cycle is measured against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is evidenced by the commissioning document. The awareness cycle is evidenced by the quarterly review notes. The third-party register is compared with the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The change process is compared with the current written standard. The risk register is evidenced by the previous year's assessment. Any deviation requires written approval and an expiry date.

The vulnerability queue is evidenced by the register of exceptions. The patch calendar is checked against the evidence pack held by the owner. The awareness cycle is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is reconciled with the ticket history for the period. The continuity plan is traced to the current written standard. The third-party register is checked against the current written standard. Any deviation requires written approval and an expiry date.

The change process is compared with the current written standard. The cloud baseline is measured against the approved design baseline. The endpoint baseline is traced to the current written standard. Any deviation requires written approval and an expiry date.

The hardened build is measured against the dependency map. The threat model is compared with the signed exception log. The metric set is traced to the most recent exercise record. The awareness cycle is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The patch calendar is reconciled with the register of exceptions. Every internet-facing service is traced to the current written standard. Records are retained only as long as the schedule requires.

The privileged access list is checked against the approved design baseline. The vulnerability queue is reviewed against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The remote access path is documented alongside the evidence pack held by the owner. The patch calendar is traced to the register of exceptions. The risk register is reconciled with the agreed service level. Each administrative account is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is evidenced by the register of exceptions. The remote access path is traced to the commissioning document. Records are retained only as long as the schedule requires.

The physical controls is compared with the dependency map. The recovery test is traced to the commissioning document. The mobile standard is evidenced by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is reconciled with the quarterly review notes. The retention schedule is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The threat model is documented alongside the evidence pack held by the owner. The segmentation boundary is reconciled with the quarterly review notes. The continuity plan is checked against the agreed service level. The intent is to make the safe path the default rather than an exception.

The physical controls is validated by the previous year's assessment. The identity lifecycle is reconciled with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is reviewed against the dependency map. The privileged access list 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 vulnerability queue is documented alongside the ticket history for the period. The classification scheme is traced to the most recent exercise record. The recovery test is evidenced by the approved design baseline. The recovery test is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The access review process is traced to the dependency map. The continuity plan is reviewed against the dependency map. Records are retained only as long as the schedule requires.

The third-party register is checked against the approved design baseline. The cloud baseline is validated by the evidence pack held by the owner. The threat model is measured against the signed exception log. The mobile standard is measured against the signed exception log. Any deviation requires written approval and an expiry date.

The mobile standard is traced to the approved design baseline. The vulnerability queue is documented alongside the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The patch calendar is compared with the most recent exercise record. The awareness cycle is checked against the signed exception log. The classification scheme is reconciled with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The remote access path is evidenced by the current written standard. The continuity plan is validated by the dependency map. The physical controls is checked against the evidence pack held by the owner. Every internet-facing service is reviewed against the signed exception log. The intent is to make the safe path the default rather than an exception.

The backup rotation is traced to the most recent exercise record. The monitoring pipeline is reconciled with the ticket history for the period. The threat model is measured against the dependency map. Any deviation requires written approval and an expiry date.

The recovery test is validated by the dependency map. The access review process is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is traced to the previous year's assessment. The awareness cycle is reconciled with the quarterly review notes. The retention schedule is validated by the signed exception log. The hardened build is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is reviewed against the commissioning document. The asset register is validated by the previous year's assessment. The retention schedule is traced to the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is compared with the previous year's assessment. The remote access path is validated by the current written standard. The patch calendar is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The threat model is compared with the previous year's assessment. The retention schedule is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

The metric set is measured against the agreed service level. The retention schedule is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

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

The risk register is validated by the agreed service level. The risk register is reconciled with the approved design baseline. The patch calendar is reviewed against the evidence pack held by the owner. The access review process is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reconciled with the ticket history for the period. The hardened build is reviewed against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is reviewed against the dependency map. The asset register is documented alongside the current written standard. The vulnerability queue is documented alongside the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The asset register is documented alongside the commissioning document. The hardened build is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

4. The continuity plan

Each administrative account is reconciled with the ticket history for the period. The hardened build is measured against the current written standard. The third-party register is reconciled with the evidence pack held by the owner. The access review process is measured against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is validated by the evidence pack held by the owner. The privileged access list is reconciled with the dependency map. The vulnerability queue is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is validated by the approved design baseline. The access review process is checked against the quarterly review notes. Every internet-facing service is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the ticket history for the period. The third-party register is evidenced by the dependency map. The endpoint baseline is compared with the most recent exercise record. The access review process is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

The continuity plan is evidenced by the signed exception log. The retention schedule is documented alongside the agreed service level. The change process is checked against the most recent exercise record. Records are retained only as long as the schedule requires.

The asset register is compared with the current written standard. The privileged access list is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is checked against the previous year's assessment. The classification scheme is documented alongside the previous year's assessment. The risk register is reconciled with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is measured against the most recent exercise record. The third-party register is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

The threat model is evidenced by the most recent exercise record. The remote access path is traced to the dependency map. The threat model is compared with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is validated by the ticket history for the period. The retention schedule is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is checked against the quarterly review notes. The backup rotation is reviewed against the signed exception log. The remote access path is evidenced by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

5. The patch calendar

The metric set is compared with the previous year's assessment. The continuity plan is compared with the commissioning document. Each administrative account is checked against the approved design baseline. The retention schedule is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The backup rotation is measured against the current written standard. The third-party register is validated by the quarterly review notes. The encryption standard is checked against the signed exception log. Records are retained only as long as the schedule requires.

The hardened build is reconciled with the dependency map. The change process is documented alongside the quarterly review notes. The mobile standard is traced to the commissioning document. The email authentication record is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The metric set is validated by the previous year's assessment. The third-party register is traced to the most recent exercise record. The backup rotation is traced to the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is documented alongside the commissioning document. The encryption standard is traced to the ticket history for the period. The retention schedule is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is measured against the quarterly review notes. The third-party register is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is traced to the previous year's assessment. The change process is evidenced by the approved design baseline. The access review process is compared with the commissioning document. The mobile standard is measured against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is traced to the quarterly review notes. The change process is documented alongside the most recent exercise record. Third parties must demonstrate the control before access is granted.

The privileged access list is measured against the agreed service level. Every internet-facing service is measured against the previous year's assessment. The access review process is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is reconciled with the agreed service level. The cloud baseline is reconciled with the current written standard. The access review process is reconciled with the previous year's assessment. The physical controls is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

6. The classification scheme

The privileged access list is measured against the agreed service level. The recovery test is checked against the current written standard. Every internet-facing service is documented alongside the dependency map. Every internet-facing service is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is compared with the most recent exercise record. Each administrative account is validated by the signed exception log. The awareness cycle is documented alongside the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is documented alongside the approved design baseline. Every internet-facing service is measured against the most recent exercise record. The threat model is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

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

The mobile standard is traced to the agreed service level. The hardened build is reconciled with the quarterly review notes. The risk register is documented alongside the previous year's assessment. The endpoint baseline is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is compared with the signed exception log. The endpoint baseline is reconciled with the previous year's assessment. The threat model is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The privileged access list is measured against the agreed service level. The privileged access list is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is traced to the most recent exercise record. The metric set 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 endpoint baseline is compared with the agreed service level. The third-party register is checked against the dependency map. The access review process is evidenced by the register of exceptions. The monitoring pipeline is traced to the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The vendor register is measured against the evidence pack held by the owner. The remote access path is reconciled with the register of exceptions. The recovery test is checked against the dependency map. The control is tested at least once every twelve months.

The patch calendar is compared with the previous year's assessment. The privileged access list is checked against the agreed service level. The vulnerability queue is validated by the commissioning document. Every internet-facing service is documented alongside the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reconciled with the commissioning document. The awareness cycle is documented alongside the register of exceptions. The privileged access list is validated by the commissioning document. The recovery test is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The remote access path is checked against the current written standard. The segmentation boundary is reviewed against the dependency map. The identity lifecycle is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

Each administrative account is evidenced by the agreed service level. The access review process is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The cloud baseline is traced to the previous year's assessment. Every internet-facing service is evidenced by the current written standard. The privileged access list is traced to the previous year's assessment. The identity lifecycle is checked against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

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

The access review process is documented alongside the quarterly review notes. The third-party register is reconciled with the signed exception log. The mobile standard is reconciled with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The awareness cycle is validated by the commissioning document. The access review process is compared with the previous year's assessment. The segmentation boundary is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is checked against the dependency map. Each administrative account is validated by the agreed service level. The intent is to make the safe path the default rather than an exception.

The change process is validated by the agreed service level. The metric set is compared with the most recent exercise record. The identity lifecycle is validated by the dependency map. Each administrative account is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The asset register is documented alongside the commissioning document. The asset register is checked against the quarterly review notes. The identity lifecycle is documented alongside the previous year's assessment. The metric set is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The encryption standard is reviewed against the ticket history for the period. The awareness cycle is reconciled with the dependency map. Each administrative account is documented alongside the current written standard. The same requirement applies to cloud services as to on-premises systems.