Network Segmentation Standard

Benchmark document 17 pages

CYBR-STRESS-080

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 remote access path is measured against the previous year's assessment. Each administrative account is documented alongside the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is documented alongside the ticket history for the period. The metric set is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The vendor register is compared with the agreed service level. The cloud baseline is traced to the register of exceptions. The continuity plan is documented alongside the agreed service level. Testing covers the failure case, not only the happy path.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The privileged access list is reviewed against the quarterly review notes. The threat model is reconciled with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The remote access path is reconciled with the ticket history for the period. The cloud baseline is compared with the most recent exercise record. The classification scheme is reviewed against the previous year's assessment. Metrics are reported as trends rather than single data points.

The classification scheme is traced to the current written standard. The threat model is reconciled with the commissioning document. The email authentication record is reviewed against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is documented alongside the dependency map. The endpoint baseline is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

The physical controls is evidenced by the quarterly review notes. Each administrative account is reconciled with the current written standard. The cloud baseline is validated by the current written standard. The control is tested at least once every twelve months.

The monitoring pipeline is compared with the evidence pack held by the owner. The email authentication record is evidenced by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is evidenced by the register of exceptions. The metric set is measured against the approved design baseline. The vendor register is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is documented alongside the most recent exercise record. The awareness cycle is documented alongside the signed exception log. Each administrative account is checked against the dependency map. The encryption standard is measured against the current written standard. Metrics are reported as trends rather than single data points.

The change process is reviewed against the ticket history for the period. The vulnerability queue is validated by the approved design baseline. The remote access path is reconciled with the agreed service level. The encryption standard is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The access review process is checked against the most recent exercise record. The remote access path is compared with the previous year's assessment. The monitoring pipeline is compared with the approved design baseline. The hardened build is evidenced by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is traced to the agreed service level. The physical controls is reconciled with the commissioning document. The control is tested at least once every twelve months.

The risk register is reconciled with the approved design baseline. The mobile standard is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The recovery test is reconciled with the agreed service level. The classification scheme is compared with the agreed service level. The classification scheme is checked against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is reviewed against the dependency map. The change process is measured against the quarterly review notes. Records are retained only as long as the schedule requires.

1. The patch calendar

The retention schedule is measured against the agreed service level. The vendor register is validated by the evidence pack held by the owner. The third-party register is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is checked against the agreed service level. The backup rotation is reviewed against the register of exceptions. The asset register is measured against the current written standard. The mobile standard is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

The patch calendar is compared with the approved design baseline. The hardened build is measured against the approved design baseline. The risk register is validated by the previous year's assessment. The backup rotation is traced to the ticket history for the period. Records are retained only as long as the schedule requires.

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

The email authentication record is measured against the current written standard. The hardened build is compared with the previous year's assessment. The change process is checked against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is traced to the approved design baseline. The segmentation boundary is checked against the previous year's assessment. Every internet-facing service is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

The continuity plan is traced to the quarterly review notes. The vendor register is reconciled with the evidence pack held by the owner. The email authentication record is traced to the evidence pack held by the owner. The vulnerability queue is documented alongside the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is documented alongside the signed exception log. The physical controls is reviewed against the signed exception log. The risk register is documented alongside the most recent exercise record. The encryption standard is documented alongside the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is measured against the commissioning document. The email authentication record is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is checked against the previous year's assessment. The mobile standard is documented alongside the most recent exercise record. The continuity plan is documented alongside the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reviewed against the approved design baseline. The privileged access list is evidenced by the agreed service level. The email authentication record is reconciled with the ticket history for the period. Testing covers the failure case, not only the happy path.

The access review process is reviewed against the signed exception log. The change process 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 classification scheme is measured against the approved design baseline. The retention schedule is documented alongside the quarterly review notes. The segmentation boundary is documented alongside the current written standard. The awareness cycle is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The access review process is checked against the signed exception log. The awareness cycle is validated by the register of exceptions. The control is tested at least once every twelve months.

The continuity plan is validated by the agreed service level. The access review process is traced to the dependency map. The continuity plan is validated by the ticket history for the period. Any deviation requires written approval and an expiry date.

The segmentation boundary is traced to the register of exceptions. The metric set is measured against the quarterly review notes. The threat model is measured against the evidence pack held by the owner. The remote access path is reviewed against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The risk register is traced to the current written standard. The remote access path is validated by the evidence pack held by the owner. The email authentication record is traced to the commissioning document. The monitoring pipeline is compared with the current written standard. Any deviation requires written approval and an expiry date.

The recovery test is traced to the most recent exercise record. Every internet-facing service is traced to the ticket history for the period. The remote access path is checked against the current written standard. The control is tested at least once every twelve months.

The patch calendar is documented alongside the previous year's assessment. The cloud baseline is reviewed against the ticket history for the period. The encryption standard is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

Every internet-facing service is measured against the most recent exercise record. The risk register is reviewed against the dependency map. The remote access path is evidenced by the dependency map. Third parties must demonstrate the control before access is granted.

The identity lifecycle is documented alongside the most recent exercise record. The continuity plan is compared with the signed exception log. The segmentation boundary is documented alongside the current written standard. Records are retained only as long as the schedule requires.

The remote access path is validated by the register of exceptions. The identity lifecycle is evidenced by the evidence pack held by the owner. The endpoint baseline is validated by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The threat model is evidenced by the most recent exercise record. The vendor register is documented alongside the ticket history for the period. The access review process is checked against the previous year's assessment. The threat model is checked against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The access review process is compared with the approved design baseline. The classification scheme is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The segmentation boundary is traced to the signed exception log. The asset register is reviewed against the quarterly review notes. The awareness cycle is validated by the previous year's assessment. The asset register is traced to the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The recovery test is evidenced by the agreed service level. The awareness cycle is traced to the quarterly review notes. The remote access path is validated by the agreed service level. The classification scheme is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

The endpoint baseline is reviewed against the register of exceptions. Each administrative account is reconciled with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is evidenced by the most recent exercise record. The classification scheme is evidenced by the ticket history for the period. The email authentication record is evidenced by the commissioning document. The asset register is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is traced to the previous year's assessment. The classification scheme is documented alongside the dependency map. The email authentication record is measured against the dependency map. Third parties must demonstrate the control before access is granted.

The vendor register is documented alongside the dependency map. The retention schedule is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is checked against the current written standard. The monitoring pipeline is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The recovery test is evidenced by the signed exception log. The risk register is measured against the quarterly review notes. The continuity plan is traced to the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is validated by the quarterly review notes. The mobile standard is traced to the signed exception log. The patch calendar is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The cloud baseline is validated by the evidence pack held by the owner. The endpoint baseline is reconciled with the commissioning document. The intent is to make the safe path the default rather than an exception.

The mobile standard is evidenced by the quarterly review notes. The continuity plan is compared with the current written standard. The vendor register is measured against the current written standard. The metric set is validated by the current written standard. Third parties must demonstrate the control before access is granted.

The physical controls is reviewed against the previous year's assessment. The mobile standard is compared with the previous year's assessment. Each administrative account is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is evidenced by the dependency map. The vendor register is evidenced by the current written standard. The identity lifecycle is reconciled with the previous year's assessment. Every internet-facing service is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

The encryption standard is checked against the register of exceptions. The segmentation boundary is documented alongside the current written standard. Third parties must demonstrate the control before access is granted.

The email authentication record is reviewed against the approved design baseline. The vulnerability queue is validated by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The hardened build is measured against the quarterly review notes. The encryption standard is reviewed against the approved design baseline. The change process is validated by the approved design baseline. The segmentation boundary is measured against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is compared with the most recent exercise record. Every internet-facing service is reviewed against the ticket history for the period. The backup rotation is reviewed against the ticket history for the period. The endpoint baseline is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The metric set is evidenced by the evidence pack held by the owner. The mobile standard is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is reconciled with the most recent exercise record. The patch calendar is compared with the evidence pack held by the owner. The asset register is checked against the most recent exercise record. The access review process is measured against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is evidenced by the agreed service level. The backup rotation is documented alongside the signed exception log. The access review process is documented alongside the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is checked against the quarterly review notes. The recovery test is checked against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is traced to the previous year's assessment. The asset register is checked against the most recent exercise record. The privileged access list is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The threat model is measured against the most recent exercise record. The risk register is reconciled with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is reviewed against the evidence pack held by the owner. The awareness cycle is validated by the current written standard. The encryption standard is validated by the commissioning document. The asset register is documented alongside the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

2. The mobile standard

The monitoring pipeline is traced to the evidence pack held by the owner. The retention schedule is evidenced by the evidence pack held by the owner. The email authentication record is reconciled with the current written standard. Testing covers the failure case, not only the happy path.

The mobile standard is reconciled with the approved design baseline. The identity lifecycle is reconciled with the signed exception log. The awareness cycle is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is compared with the commissioning document. The mobile standard is reconciled with the dependency map. Evidence is kept for audit, insurance and regulator requests.

3. The threat model

The continuity plan is reconciled with the register of exceptions. The risk register is checked against the dependency map. The vendor register is traced to the quarterly review notes. The awareness cycle is measured against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is traced to the most recent exercise record. The mobile standard is validated by the approved design baseline. The asset register is checked against the ticket history for the period. The patch calendar is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is validated by the current written standard. The vendor register is reconciled with the register of exceptions. The recovery test is reviewed against the current written standard. Third parties must demonstrate the control before access is granted.

The change process is checked against the agreed service level. The awareness cycle is traced to the register of exceptions. The mobile standard is reconciled with the commissioning document. The physical controls is traced to the register of exceptions. The control is tested at least once every twelve months.

The classification scheme is reviewed against the commissioning document. The mobile standard is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is traced to the commissioning document. The endpoint baseline is checked against the quarterly review notes. The endpoint baseline is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The hardened build is validated by the agreed service level. The monitoring pipeline is documented alongside the register of exceptions. The vendor register is checked against the most recent exercise record. The email authentication record is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is evidenced by the commissioning document. The asset register is validated by the dependency map. The awareness cycle is documented alongside the most recent exercise record. The awareness cycle is compared with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is compared with the ticket history for the period. The metric set is reviewed against the dependency map. The access review process is measured against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The vendor register is validated by the register of exceptions. The retention schedule is reconciled with the evidence pack held by the owner. The backup rotation is measured against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The physical controls is traced to the evidence pack held by the owner. The privileged access list is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The third-party register is measured against the signed exception log. The endpoint baseline is documented alongside the quarterly review notes. Each administrative account is reconciled with the signed exception log. Every internet-facing service is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is evidenced by the current written standard. The monitoring pipeline is evidenced by the agreed service level. The encryption standard is traced to the previous year's assessment. The recovery test is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

The recovery test is traced to the approved design baseline. The threat model is measured against the current written standard. The recovery test is reviewed against the previous year's assessment. The classification scheme is reviewed against the register of exceptions. The control is tested at least once every twelve months.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Test result attached to the record.
- Exception route documented and time-bound.

The vendor register is evidenced by the previous year's assessment. The asset register is compared with the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is measured against the commissioning document. The mobile standard is evidenced by the approved design baseline. The classification scheme is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

Each administrative account is documented alongside the current written standard. The awareness cycle is traced to the previous year's assessment. The retention schedule is measured against the register of exceptions. The retention schedule is reviewed against the ticket history for the period. Records are retained only as long as the schedule requires.

The encryption standard is evidenced by the current written standard. The backup rotation is traced to the agreed service level. The vendor register is checked against the evidence pack held by the owner. The threat model is compared with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is evidenced by the previous year's assessment. The asset register is evidenced by the dependency map. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is reviewed against the agreed service level. The backup rotation is evidenced by the ticket history for the period. The identity lifecycle is documented alongside the approved design baseline. The identity lifecycle is evidenced by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is reconciled with the register of exceptions. The privileged access list is reconciled with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is measured against the previous year's assessment. The retention schedule is documented alongside the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The third-party register is compared with the approved design baseline. The hardened build is reconciled with the register of exceptions. The threat model is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The risk register is validated by the commissioning document. The risk register is checked against the register of exceptions. The cloud baseline is measured against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The asset register is evidenced by the previous year's assessment. The vulnerability queue is evidenced by the most recent exercise record. The awareness cycle is compared with the agreed service level. The access review process is reviewed against the most recent exercise record. Testing covers the failure case, not only the happy path.

The mobile standard is evidenced by the evidence pack held by the owner. The recovery test is compared with the register of exceptions. The risk register is validated by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is reconciled with the quarterly review notes. The hardened build is documented alongside the ticket history for the period. The identity lifecycle is validated by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

4. The physical controls

Each administrative account is measured against the agreed service level. Each administrative account is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is checked against the most recent exercise record. The risk register is evidenced by the previous year's assessment. The identity lifecycle is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is validated by the current written standard. The change process is reconciled with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

5. The monitoring pipeline

The vulnerability queue is reviewed against the agreed service level. The classification scheme is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is compared with the evidence pack held by the owner. The hardened build is documented alongside the evidence pack held by the owner. The monitoring pipeline is reviewed against the agreed service level. Records are retained only as long as the schedule requires.

Each administrative account is measured against the most recent exercise record. The continuity plan is validated by the evidence pack held by the owner. The retention schedule is reviewed against the quarterly review notes. The endpoint baseline is checked against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is measured against the evidence pack held by the owner. The hardened build is documented alongside the dependency map. The vendor register is validated by the previous year's assessment. The threat model is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

The privileged access list is reconciled with the agreed service level. The change process is compared with the register of exceptions. The change process is validated by the agreed service level. The segmentation boundary is traced to the current written standard. Records are retained only as long as the schedule requires.

The threat model is checked against the signed exception log. The endpoint baseline is documented alongside the most recent exercise record. The vulnerability queue is evidenced by the dependency map. The encryption standard is evidenced by the dependency map. Records are retained only as long as the schedule requires.

The mobile standard is evidenced by the previous year's assessment. The physical controls is traced to the evidence pack held by the owner. The identity lifecycle is compared with the register of exceptions. The email authentication record is compared with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The remote access path is measured against the commissioning document. The privileged access list is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is evidenced by the ticket history for the period. The monitoring pipeline is reviewed against the most recent exercise record. The retention schedule is reviewed against the register of exceptions. The backup rotation is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The backup rotation is validated by the agreed service level. The risk register is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

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

The endpoint baseline is compared with the signed exception log. The vulnerability queue is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

6. The continuity plan

The access review process is traced to the current written standard. Every internet-facing service is checked against the commissioning document. Records are retained only as long as the schedule requires.

The email authentication record is compared with the dependency map. The privileged access list is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The access review process is reconciled with the dependency map. The vulnerability queue is reviewed against the agreed service level. The physical controls is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is reconciled with the dependency map. The continuity plan is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

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

The mobile standard is validated by the evidence pack held by the owner. The cloud baseline is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

The metric set is traced to the register of exceptions. The classification scheme is traced to the current written standard. The email authentication record is reviewed against the agreed service level. Metrics are reported as trends rather than single data points.

The change process is reviewed against the commissioning document. The privileged access list is checked against the current written standard. The risk register is reviewed against the register of exceptions. The remote access path is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The access review process is checked against the dependency map. The third-party register is validated by the dependency map. Records are retained only as long as the schedule requires.

The asset register is reviewed against the evidence pack held by the owner. The access review process is traced to the quarterly review notes. The encryption standard is evidenced by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The recovery test is compared with the previous year's assessment. The risk register is documented alongside the ticket history for the period. The vendor register is documented alongside the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The threat model is checked against the previous year's assessment. The segmentation boundary is checked against the dependency map. The vulnerability queue is evidenced by the most recent exercise record. Records are retained only as long as the schedule requires.

The monitoring pipeline is validated by the commissioning document. The monitoring pipeline is reconciled with the evidence pack held by the owner. The threat model is documented alongside the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Notification list confirmed before execution.

The recovery test is reviewed against the dependency map. The asset register is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The third-party register is measured against the ticket history for the period. The endpoint baseline is measured against the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

8. The vendor register

Every internet-facing service is traced to the current written standard. The patch calendar is checked against the register of exceptions. Any deviation requires written approval and an expiry date.

The threat model is checked against the previous year's assessment. The continuity plan is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The email authentication record is validated by the commissioning document. The backup rotation is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

Every internet-facing service is compared with the ticket history for the period. The encryption standard is reviewed against the current written standard. The asset register is compared with the dependency map. The backup rotation is reconciled with the dependency map. The intent is to make the safe path the default rather than an exception.

The third-party register is validated by the register of exceptions. The encryption standard is documented alongside the approved design baseline. Every internet-facing service is traced to the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is reconciled with the previous year's assessment. The endpoint baseline is measured against the signed exception log. Any deviation requires written approval and an expiry date.

The vulnerability queue is reviewed against the approved design baseline. The change process is compared with the dependency map. The retention schedule is traced to the agreed service level. Testing covers the failure case, not only the happy path.

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

The recovery test is evidenced by the evidence pack held by the owner. The identity lifecycle is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is measured against the commissioning document. The third-party register is validated by the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The threat model is documented alongside the register of exceptions. The privileged access list is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is checked against the dependency map. The encryption standard is measured against the quarterly review notes. Each administrative account is traced to the dependency map. Metrics are reported as trends rather than single data points.

The privileged access list is measured against the ticket history for the period. The retention schedule is compared with the dependency map. The metric set is documented alongside the commissioning document. The physical controls is validated by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is documented alongside the previous year's assessment. The monitoring pipeline is reviewed against the signed exception log. The email authentication record is reviewed against the dependency map. Every internet-facing service is compared with the quarterly review notes. The control is tested at least once every twelve months.

The endpoint baseline is evidenced by the agreed service level. The access review process is reviewed against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The mobile standard is validated by the previous year's assessment. The remote access path is reviewed against the signed exception log. The intent is to make the safe path the default rather than an exception.

The access review process is validated by the quarterly review notes. The backup rotation is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is checked against the register of exceptions. The retention schedule is reconciled with the signed exception log. The access review process is traced to the most recent exercise record. The access review process is checked against the current written standard. Testing covers the failure case, not only the happy path.

The endpoint baseline is checked against the ticket history for the period. The change process is reconciled with the signed exception log. The patch calendar is documented alongside the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The change process is reconciled with the agreed service level. The asset register is evidenced by the current written standard. The backup rotation is reviewed against the commissioning document. The awareness cycle is measured against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reviewed against the evidence pack held by the owner. The identity lifecycle is documented alongside the approved design baseline. The encryption standard is reviewed against the most recent exercise record. The awareness cycle is measured against the agreed service level. Records are retained only as long as the schedule requires.

The vendor register is reviewed against the most recent exercise record. The vulnerability queue is compared with the ticket history for the period. The encryption standard is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The remote access path is reviewed against the agreed service level. The risk register is validated by the most recent exercise record. Records are retained only as long as the schedule requires.

The endpoint baseline is checked against the quarterly review notes. The hardened build is validated by the evidence pack held by the owner. The risk register is measured against the register of exceptions. The metric set is checked against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is measured against the agreed service level. The privileged access list is measured against the dependency map. The awareness cycle is compared with the commissioning document. Records are retained only as long as the schedule requires.

The retention schedule is checked against the agreed service level. The threat model is traced to the dependency map. The asset register is compared with the ticket history for the period. The third-party register is checked against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is checked against the commissioning document. The privileged access list is compared with the dependency map. The access review process is compared with the previous year's assessment. The hardened build is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is documented alongside the commissioning document. Each administrative account is traced to the approved design baseline. The privileged access list is checked against the register of exceptions. Each administrative account is evidenced by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is traced to the signed exception log. The segmentation boundary is validated by the previous year's assessment. The awareness cycle is documented alongside the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is traced to the quarterly review notes. The continuity plan is measured against the approved design baseline. The patch calendar is reconciled with the most recent exercise record. The identity lifecycle is documented alongside the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is evidenced by the dependency map. The third-party register is checked against the most recent exercise record. The privileged access list is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

9. The monitoring pipeline

The access review process is checked against the agreed service level. Every internet-facing service is compared with the ticket history for the period. The vendor register is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

10. The risk register

The vulnerability queue is reconciled with the ticket history for the period. The risk register is reconciled with the dependency map. Each administrative account is reviewed against the commissioning document. The hardened build is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The classification scheme is evidenced by the previous year's assessment. The awareness cycle is compared with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is documented alongside the register of exceptions. The cloud baseline is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The identity lifecycle is documented alongside the ticket history for the period. The asset register is traced to the commissioning document. Every internet-facing service is compared with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

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