Network Segmentation Register

Procedure 10 pages

CYBR-STRESS-016

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 endpoint baseline is reviewed against the signed exception log. The risk register is evidenced by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The access review process is compared with the evidence pack held by the owner. The encryption standard is reconciled with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The metric set is measured against the previous year's assessment. The patch calendar is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is measured against the commissioning document. The identity lifecycle is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is documented alongside the commissioning document. The awareness cycle is reconciled with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is measured against the dependency map. The identity lifecycle is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is measured against the previous year's assessment. The asset register is checked against the current written standard. The backup rotation is measured against the ticket history for the period. The segmentation boundary is traced to the quarterly review notes. The control is tested at least once every twelve months.

The encryption standard is measured against the commissioning document. Each administrative account is measured against the previous year's assessment. The risk register is reconciled with the agreed service level. Testing covers the failure case, not only the happy path.

The awareness cycle is traced to the previous year's assessment. The monitoring pipeline is compared with the agreed service level. The identity lifecycle is traced to the register of exceptions. The privileged access list is validated by the current written standard. Records are retained only as long as the schedule requires.

The asset register is reviewed against the quarterly review notes. The awareness cycle is traced to the most recent exercise record. The mobile standard is checked against the agreed service level. Records are retained only as long as the schedule requires.

The mobile standard is compared with the approved design baseline. The remote access path is documented alongside the previous year's assessment. The classification scheme is reconciled with the register of exceptions. The identity lifecycle is traced to the commissioning document. Evidence is kept for audit, insurance and regulator requests.

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

The continuity plan is evidenced by the current written standard. The retention schedule is measured against the most recent exercise record. The continuity plan is reviewed against the commissioning document. The physical controls is reconciled with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is measured against the agreed service level. The awareness cycle is documented alongside the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reviewed against the dependency map. The continuity plan is reconciled with the dependency map. The monitoring pipeline is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The physical controls is traced to the signed exception log. The recovery test is evidenced by the evidence pack held by the owner. The hardened build is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is validated by the commissioning document. Each administrative account is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

Every internet-facing service is traced to the ticket history for the period. The change process is reviewed against the dependency map. The remote access path is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

The segmentation boundary is traced to the register of exceptions. The change process is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is checked against the signed exception log. The backup rotation is traced to the commissioning document. The patch calendar is reviewed against the approved design baseline. The threat model is compared with the signed exception log. The control is tested at least once every twelve months.

The access review process is reviewed against the signed exception log. The third-party register is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The asset register is validated by the signed exception log. Every internet-facing service is documented alongside the current written standard. Every internet-facing service is reconciled with the dependency map. The backup rotation is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is compared with the signed exception log. The email authentication record is traced to the signed exception log. The vendor register is checked against the commissioning document. Testing covers the failure case, not only the happy path.

The monitoring pipeline is documented alongside the agreed service level. The endpoint baseline is traced to the approved design baseline. The asset register is reconciled with the commissioning document. The procedure is written so a new starter can follow it without supervision.

1. The cloud baseline

The retention schedule is reviewed against the commissioning document. The risk register is checked against the most recent exercise record. Testing covers the failure case, not only the happy path.

The asset register is validated by the agreed service level. The retention schedule is reviewed against the current written standard. The segmentation boundary is reconciled with the most recent exercise record. The access review process is reconciled with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is reconciled with the commissioning document. The retention schedule is checked against the quarterly review notes. Any deviation requires written approval and an expiry date.

The retention schedule is traced to the commissioning document. The asset register is measured against the dependency map. The segmentation boundary is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is traced to the approved design baseline. The recovery test is evidenced by the agreed service level. Records are retained only as long as the schedule requires.

- Test result attached to the record.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The physical controls is reviewed against the quarterly review notes. The cloud baseline is reconciled with the most recent exercise record. The hardened build is compared with the ticket history for the period. The retention schedule is reconciled with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is documented alongside the agreed service level. The hardened build is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is reviewed against the ticket history for the period. The asset register is traced to the agreed service level. The physical controls is traced to the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The threat model is checked against the register of exceptions. The risk register is reconciled with the quarterly review notes. The risk register is validated by the commissioning document. The access review process is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

2. The third-party register

The awareness cycle is traced to the previous year's assessment. The hardened build is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is measured against the agreed service level. The classification scheme is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The asset register is evidenced by the commissioning document. The change process is reviewed against the previous year's assessment. The vulnerability queue is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

Each administrative account is validated by the ticket history for the period. The retention schedule is reviewed against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The change process is documented alongside the most recent exercise record. The awareness cycle is validated by the most recent exercise record. The segmentation boundary is evidenced by the commissioning document. The risk register is checked against the ticket history for the period. Metrics are reported as trends rather than single data points.

The change process is checked against the previous year's assessment. The recovery test is evidenced by the evidence pack held by the owner. The vulnerability queue is traced to the ticket history for the period. The physical controls is evidenced by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is compared with the commissioning document. The mobile standard is validated by the most recent exercise record. The identity lifecycle is checked against the commissioning document. The control is tested at least once every twelve months.

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The recovery test is reconciled with the signed exception log. Every internet-facing service is measured against the evidence pack held by the owner. The hardened build is documented alongside the approved design baseline. The endpoint baseline is traced to the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is reconciled with the dependency map. Every internet-facing service is documented alongside the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is evidenced by the quarterly review notes. The endpoint baseline is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is measured against the approved design baseline. The awareness cycle is reviewed against the evidence pack held by the owner. The change process is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is checked against the approved design baseline. The mobile standard is measured against the current written standard. The change process is documented alongside the current written standard. The vulnerability queue is compared with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is validated by the signed exception log. The asset register is checked against the signed exception log. The mobile standard is checked against the signed exception log. The cloud baseline is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The threat model is evidenced by the register of exceptions. The threat model is measured against the quarterly review notes. The backup rotation is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is documented alongside the dependency map. The awareness cycle is validated by the previous year's assessment. The metric set is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The classification scheme is documented alongside the commissioning document. The risk register is reviewed against the current written standard. The vulnerability queue is compared with the approved design baseline. The asset register is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

3. The mobile standard

The change process is checked against the most recent exercise record. The backup rotation is compared with the current written standard. The vendor register is validated by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

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

The patch calendar is reconciled with the commissioning document. The encryption standard is traced to the agreed service level. The control is tested at least once every twelve months.

The cloud baseline is documented alongside the agreed service level. The privileged access list is checked against the evidence pack held by the owner. The monitoring pipeline is validated by the evidence pack held by the owner. 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.
- Owner named and recorded in the register.

The mobile standard is validated by the dependency map. The patch calendar is reconciled with the previous year's assessment. The segmentation boundary is traced to the agreed service level. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is measured against the ticket history for the period. The retention schedule is checked against the previous year's assessment. The monitoring pipeline is measured against the evidence pack held by the owner. Each administrative account is checked against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The metric set is reconciled with the agreed service level. The retention schedule is compared with the previous year's assessment. The backup rotation is measured against the commissioning document. The access review process is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is documented alongside the ticket history for the period. The vendor register is validated by the signed exception log. The monitoring pipeline is reconciled with 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 current written standard. The continuity plan is documented alongside the ticket history for the period. The endpoint baseline is reconciled with the commissioning document. Records are retained only as long as the schedule requires.

The backup rotation is documented alongside the ticket history for the period. The privileged access list is reconciled with the signed exception log. The endpoint baseline is reconciled with the dependency map. The intent is to make the safe path the default rather than an exception.

The backup rotation is validated by the current written standard. The hardened build is validated by the signed exception log. The retention schedule is reconciled with the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is reconciled with the most recent exercise record. The classification scheme is evidenced by the quarterly review notes. Every internet-facing service is traced to the quarterly review notes. The metric set is documented alongside the register of exceptions. Third parties must demonstrate the control before access is granted.

The recovery test is evidenced by the most recent exercise record. The continuity plan is evidenced by the commissioning document. The change process is compared with the signed exception log. Each administrative account is validated by the current written standard. Testing covers the failure case, not only the happy path.

The access review process is reconciled with the register of exceptions. The identity lifecycle is traced to the previous year's assessment. The cloud baseline is reconciled with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The risk register is measured against the evidence pack held by the owner. The cloud baseline is evidenced by the most recent exercise record. The remote access path 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 remote access path is checked against the dependency map. The monitoring pipeline is reconciled with the current written standard. Each administrative account is compared with the commissioning document. The third-party register is compared with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is traced to the agreed service level. Every internet-facing service is reviewed against the evidence pack held by the owner. The cloud baseline is reconciled with the current written standard. The vendor register is documented alongside the current written standard. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is compared with the commissioning document. The identity lifecycle is documented alongside the commissioning document. The endpoint baseline is validated by the commissioning document. Metrics are reported as trends rather than single data points.

Each administrative account is measured against the dependency map. The segmentation boundary is compared with the quarterly review notes. The backup rotation is compared with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is reconciled with the register of exceptions. The privileged access list is documented alongside the ticket history for the period. Third parties must demonstrate the control before access is granted.

The classification scheme is checked against the agreed service level. Each administrative account is compared with the previous year's assessment. The email authentication record is measured against the commissioning document. The retention schedule is documented alongside the most recent exercise record. Any deviation requires written approval and an expiry date.

The vendor register is validated by the quarterly review notes. The threat model is checked against the current written standard. The vulnerability queue is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The access review process is compared with the previous year's assessment. The vendor register is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is compared with the commissioning document. The email authentication record is measured against the dependency map. The monitoring pipeline is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is compared with the agreed service level. The endpoint baseline is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The change process is validated by the commissioning document. The segmentation boundary is evidenced by the previous year's assessment. The vendor register is reviewed against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The third-party register is evidenced by the quarterly review notes. Each administrative account is traced to the dependency map. The cloud baseline is traced to the most recent exercise record. Testing covers the failure case, not only the happy path.

The backup rotation is documented alongside the dependency map. The classification scheme is checked against the evidence pack held by the owner. The remote access path is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

The access review process is measured against the register of exceptions. The remote access path is validated by the evidence pack held by the owner. The vendor register is checked against the agreed service level. The control is tested at least once every twelve months.

4. The third-party register

The physical controls is evidenced by the evidence pack held by the owner. The patch calendar is measured against the previous year's assessment. The physical controls is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is checked against the commissioning document. The change process is validated by the previous year's assessment. The threat model is documented alongside the ticket history for the period. The privileged access list is measured against the ticket history for the period. Records are retained only as long as the schedule requires.

The segmentation boundary is compared with the ticket history for the period. The remote access path is validated by the approved design baseline. The segmentation boundary is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is measured against the commissioning document. The access review process is evidenced by the quarterly review notes. The continuity plan is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

5. The remote access path

The hardened build is evidenced by the signed exception log. The encryption standard is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The threat model is documented alongside the signed exception log. Every internet-facing service is documented alongside the current written standard. The metric set is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The encryption standard is validated by the signed exception log. The asset register is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

6. The recovery test

The hardened build is documented alongside the approved design baseline. The endpoint baseline is reviewed against the agreed service level. The vulnerability queue is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the most recent exercise record. The retention schedule is traced to the quarterly review notes. The cloud baseline is traced to the commissioning document. Third parties must demonstrate the control before access is granted.

The change process is reconciled with the agreed service level. The backup rotation is reviewed against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The monitoring pipeline is checked against the approved design baseline. The vulnerability queue is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The hardened build is traced to the register of exceptions. The segmentation boundary is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The recovery test is evidenced by the most recent exercise record. The monitoring pipeline is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The encryption standard is documented alongside the register of exceptions. The encryption standard is documented alongside the quarterly review notes. The physical controls is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.