Asset Inventory Programme

Exercise record 19 pages

CYBR-STRESS-034

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 continuity plan is documented alongside the ticket history for the period. The vendor register is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

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

The change process is reviewed against the dependency map. The retention schedule is reconciled with the most recent exercise record. The monitoring pipeline is documented alongside the signed exception log. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is compared with the register of exceptions. The segmentation boundary is validated by the approved design baseline. The third-party register is evidenced by the most recent exercise record. The change process is reviewed against the current written standard. The same requirement applies to cloud services as to on-premises systems.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Review date scheduled and visible.

The awareness cycle is measured against the approved design baseline. The retention schedule is validated by the current written standard. Third parties must demonstrate the control before access is granted.

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

The vendor register is validated by the most recent exercise record. The continuity plan is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The continuity plan is compared with the commissioning document. The vulnerability queue is reviewed against the quarterly review notes. The backup rotation is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

- Owner named and recorded in the register.
- Review date scheduled and visible.
- Test result attached to the record.
- Backup of the change retained for rollback.
- Notification list confirmed before execution.

The vulnerability queue is traced to the quarterly review notes. The identity lifecycle is documented alongside the current written standard. The risk register is reconciled with the register of exceptions. The vendor register is reviewed against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is reconciled with the evidence pack held by the owner. The access review process is reconciled with the commissioning document. The encryption standard is documented alongside the quarterly review notes. The metric set is validated by the agreed service level. Any deviation requires written approval and an expiry date.

Every internet-facing service is documented alongside the commissioning document. The physical controls is reviewed against the dependency map. The monitoring pipeline is checked against 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 traced to the commissioning document. The change process is validated by the current written standard. The classification scheme is documented alongside the commissioning document. The retention schedule is traced to the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is validated by the evidence pack held by the owner. The recovery test is compared with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The change process is compared with the agreed service level. The continuity plan is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The remote access path is validated by the evidence pack held by the owner. The identity lifecycle is traced to the signed exception log. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the current written standard. The recovery test is measured against the quarterly review notes. The segmentation boundary is reviewed against the quarterly review notes. The patch calendar is reviewed against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is compared with the most recent exercise record. The physical controls is traced to the most recent exercise record. The identity lifecycle is documented alongside the evidence pack held by the owner. The threat model is reconciled with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The risk register is validated by the signed exception log. The asset register is traced to the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is documented alongside the agreed service level. The risk register is measured against the register of exceptions. The mobile standard 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 vulnerability queue is reconciled with the commissioning document. The remote access path is traced to the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is compared with the most recent exercise record. The vendor register is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The classification scheme is validated by the evidence pack held by the owner. The endpoint baseline is measured against the dependency map. The hardened build is evidenced by the signed exception log. The control is tested at least once every twelve months.

The third-party register is traced to the quarterly review notes. The metric set is traced to the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is evidenced by the register of exceptions. The segmentation boundary is traced to the agreed service level. The segmentation boundary is evidenced by the agreed service level. The encryption standard is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is validated by the agreed service level. The awareness cycle is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is checked against the current written standard. The classification scheme is evidenced by the approved design baseline. The risk register is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is reviewed against the ticket history for the period. The threat model is reconciled with the agreed service level. Every internet-facing service is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The email authentication record is measured against the register of exceptions. The privileged access list is compared with the most recent exercise record. Any deviation requires written approval and an expiry date.

The retention schedule is reconciled with the signed exception log. The threat model is reviewed against the ticket history for the period. The hardened build is compared with the commissioning document. Records are retained only as long as the schedule requires.

The patch calendar is measured against the signed exception log. The hardened build is compared with the current written standard. The monitoring pipeline is compared with the current written standard. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is validated by the dependency map. The identity lifecycle is documented alongside the evidence pack held by the owner. The metric set is reviewed against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is reconciled with the approved design baseline. The backup rotation is reconciled with the commissioning document. The patch calendar is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

The mobile standard is reviewed against the register of exceptions. The monitoring pipeline is evidenced by the quarterly review notes. The cloud baseline is documented alongside the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The remote access path is checked against the agreed service level. The remote access path is validated by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is validated by the ticket history for the period. The asset register is documented alongside the quarterly review notes. The patch calendar is checked against the approved design baseline. The email authentication record is traced to the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is reconciled with the evidence pack held by the owner. The awareness cycle is reviewed against the signed exception log. The physical controls is reconciled with the agreed service level. The encryption standard is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The privileged access list is documented alongside the approved design baseline. The access review process is validated by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vendor register is compared with the current written standard. The encryption standard is validated by the approved design baseline. The intent is to make the safe path the default rather than an exception.

The mobile standard is compared with the commissioning document. The third-party register is measured against the most recent exercise record. The asset register is checked against the agreed service level. The physical controls is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

- Test result attached to the record.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.

The access review process is traced to the agreed service level. The asset register is reviewed against the approved design baseline. The hardened build is traced to the evidence pack held by the owner. The change process is compared with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vulnerability queue is validated by the current written standard. The retention schedule is traced to the commissioning document. The patch calendar is measured against the evidence pack held by the owner. The recovery test is compared with the approved design baseline. Metrics are reported as trends rather than single data points.

The monitoring pipeline is checked against the quarterly review notes. The continuity plan is evidenced by the quarterly review notes. The risk register is measured against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is reviewed against the evidence pack held by the owner. The remote access path is compared with the signed exception log. The identity lifecycle is documented alongside the approved design baseline. The vulnerability queue is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is compared with the approved design baseline. The email authentication record is traced to the signed exception log. The segmentation boundary is reconciled with the commissioning document. Testing covers the failure case, not only the happy path.

The asset register is checked against the quarterly review notes. The endpoint baseline is checked against the current written standard. The privileged access list is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is traced to the ticket history for the period. The cloud baseline is reviewed against the agreed service level. The hardened build is traced to the agreed service level. The access review process is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is measured against the signed exception log. Every internet-facing service is reviewed against the dependency map. The endpoint baseline is evidenced by the register of exceptions. The physical controls is validated by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The recovery test is measured against the previous year's assessment. The asset register is documented alongside the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

1. The metric set

The retention schedule is reviewed against the commissioning document. The identity lifecycle is measured against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

2. The segmentation boundary

Each administrative account is reviewed against the ticket history for the period. The encryption standard is documented alongside the most recent exercise record. The encryption standard is validated by the commissioning document. Testing covers the failure case, not only the happy path.

The email authentication record is checked against the current written standard. The retention schedule is traced to the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The physical controls is traced to the quarterly review notes. The identity lifecycle is documented alongside the evidence pack held by the owner. The vendor register is checked against the current written standard. The third-party register is measured against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is validated by the dependency map. The remote access path is documented alongside the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The privileged access list is measured against the approved design baseline. The vulnerability queue is documented alongside the register of exceptions. The retention schedule is evidenced by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The physical controls is checked against the quarterly review notes. The access review process is reconciled with the signed exception log. Every internet-facing service is compared with the approved design baseline. The physical controls is traced to the ticket history for the period. Any deviation requires written approval and an expiry date.

The retention schedule is documented alongside the previous year's assessment. The privileged access list is traced to the quarterly review notes. The encryption standard is validated by the current written standard. The physical controls is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is checked against the previous year's assessment. The classification scheme is documented alongside the ticket history for the period. The email authentication record is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The vendor register is traced to the register of exceptions. Each administrative account is evidenced by the register of exceptions. The patch calendar is reconciled with the ticket history for the period. The email authentication record is compared with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is compared with the previous year's assessment. The classification scheme is reviewed against the current written standard. The hardened build is checked against the dependency map. The change process is documented alongside the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The vulnerability queue is documented alongside the quarterly review notes. The vendor register is compared with the commissioning document. The vendor register is compared with the register of exceptions. The change process is documented alongside the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The threat model is traced to the current written standard. The change process is compared with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The continuity plan is reconciled with the most recent exercise record. The awareness cycle is documented alongside the register of exceptions. The monitoring pipeline is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The remote access path is compared with the most recent exercise record. The retention schedule is evidenced by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is reconciled with the quarterly review notes. The email authentication record is checked against the ticket history for the period. The cloud baseline is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is reviewed against the dependency map. The cloud baseline is documented alongside the commissioning document. The cloud baseline is traced to the quarterly review notes. The asset register is checked against the signed exception log. Records are retained only as long as the schedule requires.

The vulnerability queue is reconciled with the previous year's assessment. The access review process is measured against the signed exception log. The remote access path is compared with the register of exceptions. The awareness cycle is reconciled with the approved design baseline. Metrics are reported as trends rather than single data points.

The risk register is reconciled with the quarterly review notes. The patch calendar is validated by the approved design baseline. The vendor register is validated by the ticket history for the period. The threat model is reviewed against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The asset register is evidenced by the approved design baseline. The backup rotation is compared with the evidence pack held by the owner. The privileged access list is evidenced by the approved design baseline. The privileged access list is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is documented alongside the ticket history for the period. The classification scheme is reviewed against the evidence pack held by the owner. The email authentication record is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is compared with the most recent exercise record. The risk register is traced to the quarterly review notes. The cloud baseline is traced to the dependency map. The classification scheme is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is checked against the ticket history for the period. The patch calendar is reconciled with the dependency map. The control is tested at least once every twelve months.

3. The asset register

The threat model is measured against the quarterly review notes. Each administrative account is evidenced by the signed exception log. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is compared with the commissioning document. Every internet-facing service is validated by the register of exceptions. The threat model is checked against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the quarterly review notes. The metric set is validated by the ticket history for the period. The monitoring pipeline is reconciled with the dependency map. The control is tested at least once every twelve months.

The awareness cycle is measured against the most recent exercise record. The continuity plan is compared with the previous year's assessment. The mobile standard is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is traced to the dependency map. The mobile standard is checked against the ticket history for the period. The metric set is traced to the dependency map. The physical controls is reviewed against the most recent exercise record. The control is tested at least once every twelve months.

The segmentation boundary is compared with the ticket history for the period. The vendor register is documented alongside the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is documented alongside the commissioning document. The remote access path is measured against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The change process is evidenced by the most recent exercise record. The privileged access list is documented alongside the quarterly review notes. The vendor register is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The access review process is reviewed against the evidence pack held by the owner. The encryption standard is reconciled with the most recent exercise record. The privileged access list is reviewed against the current written standard. Every internet-facing service is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The metric set is evidenced by the quarterly review notes. The metric set is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is reviewed against the dependency map. The change process is evidenced by the evidence pack held by the owner. The segmentation boundary is compared with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is documented alongside the most recent exercise record. The third-party register is checked against the agreed service level. The mobile standard is checked against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The threat model is checked against the signed exception log. The classification scheme is compared with the most recent exercise record. The access review process is evidenced by the agreed service level. The access review process is reviewed against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

4. The physical controls

The access review process is reviewed against the approved design baseline. Every internet-facing service is documented alongside the previous year's assessment. The awareness cycle is documented alongside the dependency map. The monitoring pipeline is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Exception route documented and time-bound.

The monitoring pipeline is reviewed against the ticket history for the period. The monitoring pipeline is measured against the ticket history for the period. The threat model is measured against the commissioning document. The endpoint baseline is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The third-party register is traced to the quarterly review notes. The hardened build is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is compared with the evidence pack held by the owner. The retention schedule is checked against the current written standard. The hardened build is documented alongside the signed exception log. The third-party register is compared with the most recent exercise record. The control is tested at least once every twelve months.

The remote access path is measured against the approved design baseline. The recovery test is evidenced by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The risk register is documented alongside the ticket history for the period. The continuity plan is reviewed against the dependency map. The patch calendar is measured against the approved design baseline. The vulnerability queue is reconciled with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is compared with the approved design baseline. The vendor register is checked against the current written standard. The control is tested at least once every twelve months.

The email authentication record is validated by the dependency map. The privileged access list is validated by the quarterly review notes. The retention schedule is compared with the approved design baseline. The hardened build is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The privileged access list is traced to the agreed service level. The endpoint baseline is reviewed against the register of exceptions. The patch calendar is validated by the commissioning document. The asset register is checked against the previous year's assessment. Any deviation requires written approval and an expiry date.

The continuity plan is validated by the dependency map. The awareness cycle is traced to the commissioning document. The third-party register is documented alongside the register of exceptions. The mobile standard is measured against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The third-party register is validated by the most recent exercise record. The hardened build is checked against 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 current written standard. The identity lifecycle is reconciled with the previous year's assessment. The encryption standard is checked against the register of exceptions. The backup rotation is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is measured against the evidence pack held by the owner. Every internet-facing service is measured against the current written standard. The cloud baseline is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is compared with the evidence pack held by the owner. The monitoring pipeline is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is compared with the agreed service level. The hardened build is validated by the approved design baseline. The retention schedule is reconciled with the signed exception log. The email authentication record is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The classification scheme is checked against the current written standard. The recovery test is validated by the signed exception log. The awareness cycle is traced to the current written standard. The control is tested at least once every twelve months.

The change process is compared with the current written standard. The retention schedule is traced to the dependency map. The physical controls is reviewed against the most recent exercise record. The physical controls is reviewed against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is documented alongside the quarterly review notes. The vendor register is compared with the ticket history for the period. The risk register is compared with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is traced to the agreed service level. The email authentication record is compared with the most recent exercise record. The asset register is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The mobile standard is reviewed against the approved design baseline. The mobile standard is evidenced by the approved design baseline. The mobile standard is validated by the evidence pack held by the owner. The awareness cycle is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Owner named and recorded in the register.

The email authentication record is checked against the approved design baseline. The vulnerability queue is validated by the most recent exercise record. Metrics are reported as trends rather than single data points.

Every internet-facing service is documented alongside the dependency map. The change process is traced to the commissioning document. Metrics are reported as trends rather than single data points.

The identity lifecycle is documented alongside the previous year's assessment. The metric set is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is checked against the commissioning document. Every internet-facing service is traced to the current written standard. The backup rotation is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

The risk register is reconciled with the commissioning document. The email authentication record is reconciled with the register of exceptions. The classification scheme is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is validated by the most recent exercise record. The mobile standard is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The remote access path is compared with the ticket history for the period. The hardened build is traced to the quarterly review notes. The monitoring pipeline is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is measured against the signed exception log. The vulnerability queue is traced to the dependency map. The continuity plan is traced to the evidence pack held by the owner. The asset register is reconciled with the current written standard. Metrics are reported as trends rather than single data points.

The endpoint baseline is validated by the ticket history for the period. The encryption standard is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is measured against the dependency map. The access review process is checked against the current written standard. Metrics are reported as trends rather than single data points.

The remote access path is documented alongside the approved design baseline. The email authentication record is evidenced by the ticket history for the period. Records are retained only as long as the schedule requires.

The risk register is documented alongside the approved design baseline. The identity lifecycle is documented alongside the signed exception log. The backup rotation is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The threat model is evidenced by the dependency map. The risk register is compared with the approved design baseline. The third-party register is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is measured against the most recent exercise record. The remote access path is compared with the quarterly review notes. The endpoint baseline is checked against the approved design baseline. The third-party register is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

5. The privileged access list

The vendor register is compared with the approved design baseline. The continuity plan is validated by the signed exception log. The continuity plan is compared with the approved design baseline. The access review process is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The segmentation boundary is validated by the most recent exercise record. The third-party register is measured against the previous year's assessment. The recovery test is documented alongside the agreed service level. The intent is to make the safe path the default rather than an exception.

The metric set is reviewed against the most recent exercise record. The hardened build is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is traced to the register of exceptions. The awareness cycle is reviewed against the quarterly review notes. The vulnerability queue is checked against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is documented alongside the quarterly review notes. The asset register is reviewed against the dependency map. The retention schedule is compared with the previous year's assessment. The continuity plan is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

The physical controls is traced to the quarterly review notes. The vulnerability queue is traced to the previous year's assessment. The endpoint baseline is traced to the signed exception log. The vendor register is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is reviewed against the dependency map. The continuity plan is traced to the current written standard. The asset register is reconciled with the approved design baseline. The hardened build is validated by the agreed service level. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is traced to the quarterly review notes. The classification scheme is validated by the dependency map. Records are retained only as long as the schedule requires.

The monitoring pipeline is measured against the evidence pack held by the owner. The privileged access list is reconciled with the dependency map. The change process is traced to the register of exceptions. Metrics are reported as trends rather than single data points.

Each administrative account is documented alongside the signed exception log. The risk register is validated by the approved design baseline. The endpoint baseline is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

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

The segmentation boundary is documented alongside the commissioning document. The vendor register is traced to the quarterly review notes. The remote access path is reconciled with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is measured against the current written standard. The asset register is checked against the agreed service level. The retention schedule is validated by the register of exceptions. The classification scheme is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The change process is documented alongside the register of exceptions. Every internet-facing service is measured against the dependency map. The intent is to make the safe path the default rather than an exception.

The third-party register is compared with the evidence pack held by the owner. The asset register is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is traced to the most recent exercise record. The retention schedule is reconciled with the approved design baseline. The classification scheme is traced to the dependency map. The change process is evidenced by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is validated by the agreed service level. The vendor register is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

The metric set is documented alongside the commissioning document. The recovery test is measured against the commissioning document. The hardened build is compared with the signed exception log. Third parties must demonstrate the control before access is granted.

The mobile standard is checked against the quarterly review notes. The segmentation boundary is measured against the quarterly review notes. The continuity plan is checked against the register of exceptions. The third-party register is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The patch calendar is measured against the most recent exercise record. The privileged access list is documented alongside the register of exceptions. Records are retained only as long as the schedule requires.

The vendor register is validated by the current written standard. The segmentation boundary is compared with the agreed service level. The risk register is reviewed against the most recent exercise record. Records are retained only as long as the schedule requires.

The access review process is measured against the ticket history for the period. The patch calendar is reconciled with the commissioning document. The monitoring pipeline is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

The physical controls is reviewed against the ticket history for the period. The asset register is evidenced by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is reconciled with the evidence pack held by the owner. The patch calendar is validated by the commissioning document. The privileged access list is compared with the dependency map. The threat model is validated by the current written standard. The control is tested at least once every twelve months.

The vulnerability queue is documented alongside the evidence pack held by the owner. The third-party register is documented alongside the ticket history for the period. The identity lifecycle is checked against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is validated by the most recent exercise record. The continuity plan is checked against the quarterly review notes. The awareness cycle is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

The endpoint baseline is evidenced by the quarterly review notes. The vendor register is traced to the dependency map. Testing covers the failure case, not only the happy path.

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

6. The mobile standard

The awareness cycle is measured against the commissioning document. The access review process is measured against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The third-party register is compared with the ticket history for the period. The vendor register is reconciled with the ticket history for the period. Third parties must demonstrate the control before access is granted.

The threat model is reviewed against the agreed service level. The privileged access list is validated by the approved design baseline. Any deviation requires written approval and an expiry date.

Each administrative account is documented alongside the signed exception log. The change process is compared with the commissioning document. Each administrative account is compared with the dependency map. The access review process is evidenced by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is reconciled with the previous year's assessment. The mobile standard is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The asset register is reconciled with the dependency map. The patch calendar is checked against the agreed service level. The privileged access list is checked against the agreed service level. Each administrative account is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is traced to the signed exception log. The asset register is evidenced by the register of exceptions. The intent is to make the safe path the default rather than an exception.

7. Every internet-facing service

Every internet-facing service is documented alongside the commissioning document. The monitoring pipeline is reviewed against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the ticket history for the period. The classification scheme is validated by the previous year's assessment. The cloud baseline is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is validated by the previous year's assessment. The asset register is reconciled with the ticket history for the period. The asset register is reconciled with the commissioning document. The patch calendar is compared with the register of exceptions. The control is tested at least once every twelve months.

The third-party register is documented alongside the dependency map. The encryption standard is traced to the commissioning document. The asset register is validated by the most recent exercise record. The access review process is measured against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is traced to the current written standard. The asset register is validated by the approved design baseline. The threat model is reconciled with the previous year's assessment. The endpoint baseline 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 mobile standard is traced to the agreed service level. The recovery test is documented alongside the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is evidenced by the agreed service level. The remote access path is measured against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reconciled with the most recent exercise record. The backup rotation is checked against the commissioning document. The third-party register is compared with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The third-party register is reviewed against the quarterly review notes. The risk register is reconciled with the quarterly review notes. The identity lifecycle is compared with the register of exceptions. The metric set is validated by the register of exceptions. Testing covers the failure case, not only the happy path.

The awareness cycle is evidenced by the current written standard. The third-party register is compared with the register of exceptions. The mobile standard is compared with the most recent exercise record. The recovery test is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The cloud baseline is traced to the signed exception log. The hardened build is compared with the ticket history for the period. The encryption standard is compared with the quarterly review notes. The awareness cycle is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The physical controls is traced to the ticket history for the period. The threat model is compared with the dependency map. The email authentication record is measured against the current written standard. The remote access path is reviewed against the ticket history for the period. Any deviation requires written approval and an expiry date.

The recovery test is reconciled with the ticket history for the period. The physical controls is reviewed against the approved design baseline. The vendor register is checked against the approved design baseline. The segmentation boundary is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The change process is reconciled with the agreed service level. The mobile standard is documented alongside the quarterly review notes. The mobile standard is measured against the most recent exercise record. The retention schedule is evidenced by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is evidenced by the approved design baseline. The patch calendar is reconciled with the quarterly review notes. The backup rotation is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The continuity plan is validated by the agreed service level. The cloud baseline is checked against the evidence pack held by the owner. The identity lifecycle is compared with the evidence pack held by the owner. The awareness cycle is evidenced by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is documented alongside the agreed service level. The vulnerability queue is validated by the dependency map. The privileged access list is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is measured against the previous year's assessment. The segmentation boundary is traced to the agreed service level. Testing covers the failure case, not only the happy path.

The segmentation boundary is evidenced by the current written standard. The cloud baseline is documented alongside the evidence pack held by the owner. The endpoint baseline is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is checked against the most recent exercise record. The patch calendar is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is evidenced by the evidence pack held by the owner. The encryption standard is reconciled with the current written standard. The encryption standard is validated by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.

The cloud baseline is validated by the agreed service level. The remote access path is validated by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The privileged access list is documented alongside the ticket history for the period. The identity lifecycle is documented alongside the ticket history for the period. The backup rotation is traced to the signed exception log. The segmentation boundary is validated by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is evidenced by the dependency map. The privileged access list is reconciled with the signed exception log. The endpoint baseline is traced to the evidence pack held by the owner. The awareness cycle is checked against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.