Data Retention Programme

Assessment report 17 pages

CYBR-STRESS-032

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.

1. The patch calendar

The cloud baseline is compared with the previous year's assessment. The encryption standard is reconciled with the most recent exercise record. The awareness cycle is traced to the signed exception log. The classification scheme is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is evidenced by the register of exceptions. The remote access path is evidenced by the evidence pack held by the owner. The retention schedule is validated by the current written standard. The continuity plan is evidenced by the agreed service level. The intent is to make the safe path the default rather than an exception.

The access review process is checked against the previous year's assessment. The email authentication record is checked against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The threat model is validated by the commissioning document. The encryption standard is traced to the commissioning document. The metric set is measured against the agreed service level. The endpoint baseline is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is evidenced by the ticket history for the period. Each administrative account is reconciled with the signed exception log. The identity lifecycle is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The risk register is documented alongside the previous year's assessment. The awareness cycle is evidenced by the dependency map. The identity lifecycle is compared with the previous year's assessment. Each administrative account is checked against the previous year's assessment. Testing covers the failure case, not only the happy path.

2. The vulnerability queue

The identity lifecycle is checked against the dependency map. The retention schedule is validated by the evidence pack held by the owner. The awareness cycle is validated by the evidence pack held by the owner. Every internet-facing service is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is validated by the register of exceptions. The awareness cycle is evidenced by the dependency map. Testing covers the failure case, not only the happy path.

The privileged access list is checked against the ticket history for the period. The metric set is measured against the ticket history for the period. The vulnerability queue is checked against the current written standard. The endpoint baseline is compared with the commissioning document. Third parties must demonstrate the control before access is granted.

The awareness cycle is checked against the quarterly review notes. The monitoring pipeline is reviewed against the commissioning document. The identity lifecycle is evidenced by the approved design baseline. The segmentation boundary is evidenced by the quarterly review notes. Any deviation requires written approval and an expiry date.

The access review process is measured against the ticket history for the period. The vendor register is traced to the agreed service level. Testing covers the failure case, not only the happy path.

The classification scheme is validated by the agreed service level. Every internet-facing service is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

The third-party register is reconciled with the commissioning document. The change process is evidenced by the current written standard. The control is tested at least once every twelve months.

The email authentication record is measured against the dependency map. The encryption standard is reconciled with the most recent exercise record. The remote access path is reconciled with the ticket history for the period. The privileged access list is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is checked against the quarterly review notes. The email authentication record is validated by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is validated by the signed exception log. The asset register is documented alongside the previous year's assessment. The privileged access list is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is documented alongside the agreed service level. The monitoring pipeline is evidenced by the approved design baseline. The privileged access list is traced to the agreed service level. The recovery test is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

The physical controls is validated by the approved design baseline. The vendor register is compared with the quarterly review notes. The email authentication record is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

The privileged access list is reviewed against the approved design baseline. The access review process is documented alongside the ticket history for the period. The segmentation boundary is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The monitoring pipeline is validated by the evidence pack held by the owner. Each administrative account is compared with the commissioning document. Third parties must demonstrate the control before access is granted.

The identity lifecycle is validated by the commissioning document. The vendor register is measured against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is validated by the previous year's assessment. The metric set is reviewed against the current written standard. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is checked against the register of exceptions. The vendor register is compared with the dependency map. The metric set is traced to the quarterly review notes. The retention schedule is reconciled with the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is documented alongside the previous year's assessment. The recovery test is evidenced by the signed exception log. The email authentication record is traced to the approved design baseline. The threat model is measured against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is measured against the previous year's assessment. The awareness cycle is traced to the previous year's assessment. The access review process is compared with the most recent exercise record. Testing covers the failure case, not only the happy path.

The metric set is measured against the most recent exercise record. The change process is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The patch calendar is validated by the current written standard. The vulnerability queue is checked against the register of exceptions. The email authentication record is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The change process is documented alongside the evidence pack held by the owner. The awareness cycle is reviewed against the commissioning document. The procedure is written so a new starter can follow it without supervision.

- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Exception route documented and time-bound.
- Test result attached to the record.

The email authentication record is measured against the register of exceptions. The monitoring pipeline is evidenced by the ticket history for the period. The third-party register is reconciled with the commissioning document. The recovery test is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is traced to the ticket history for the period. The cloud baseline is checked against the previous year's assessment. Testing covers the failure case, not only the happy path.

The continuity plan is reviewed against the approved design baseline. The continuity plan is measured against the evidence pack held by the owner. The segmentation boundary is validated by the register of exceptions. The classification scheme is evidenced by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

3. The backup rotation

The vulnerability queue is measured against the most recent exercise record. The third-party register is checked against the ticket history for the period. The awareness cycle is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

4. The remote access path

The monitoring pipeline is evidenced by the commissioning document. The hardened build is measured against the register of exceptions. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.

The remote access path is measured against the most recent exercise record. The classification scheme is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The hardened build is checked against the quarterly review notes. The threat model is reviewed against the ticket history for the period. The physical controls is traced to the dependency map. The continuity plan is reviewed against the current written standard. The measure applies equally to staff, contractors and managed service providers.

The physical controls is documented alongside the agreed service level. The risk register is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

The change process is reviewed against the current written standard. The threat model is traced to the agreed service level. The continuity plan is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is reconciled with the commissioning document. The endpoint baseline is reviewed against the commissioning document. The continuity plan is evidenced by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The third-party register is checked against the ticket history for the period. The physical controls is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is compared with the commissioning document. The asset register is measured against the ticket history for the period. The remote access path is validated by the dependency map. The vulnerability queue is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

The mobile standard is reconciled with the signed exception log. The asset register is documented alongside the agreed service level. The change process is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The continuity plan is measured against the register of exceptions. The segmentation boundary is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The change process is traced to the agreed service level. The email authentication record is measured against the previous year's assessment. Any deviation requires written approval and an expiry date.

The physical controls is documented alongside the evidence pack held by the owner. The cloud baseline is documented alongside the commissioning document. The physical controls is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

5. The awareness cycle

The privileged access list is traced to the quarterly review notes. The mobile standard is checked against the approved design baseline. The metric set is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is documented alongside the quarterly review notes. The change process is reconciled with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The metric set is checked against the quarterly review notes. The retention schedule is compared with the dependency map. Records are retained only as long as the schedule requires.

The asset register is traced to the quarterly review notes. The monitoring pipeline is measured against the ticket history for the period. Every internet-facing service is measured against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The access review process is evidenced by the commissioning document. The third-party register is evidenced by the dependency map. The change process is reviewed against the agreed service level. Each administrative account is validated by the approved design baseline. Metrics are reported as trends rather than single data points.

The third-party register is reconciled with the most recent exercise record. The endpoint baseline is validated by the ticket history for the period. The recovery test is traced to the most recent exercise record. The metric set is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is measured against the dependency map. The awareness cycle is compared with the register of exceptions. The remote access path is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

The asset register is evidenced by the ticket history for the period. The email authentication record is evidenced by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is checked against the signed exception log. The endpoint baseline is evidenced by the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The metric set is documented alongside the previous year's assessment. The patch calendar is checked against the most recent exercise record. The patch calendar is reconciled with the most recent exercise record. The threat model is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is evidenced by the quarterly review notes. The hardened build is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is traced to the evidence pack held by the owner. The third-party register is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The asset register is validated by the evidence pack held by the owner. The backup rotation is validated by the signed exception log. The vulnerability queue is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The vendor register is reconciled with the evidence pack held by the owner. The risk register is reviewed against the signed exception log. The continuity plan is reviewed against the approved design baseline. The mobile standard is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The access review process is measured against the quarterly review notes. The threat model is traced to the dependency map. The mobile standard is reconciled with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The third-party register is checked against the dependency map. The continuity plan is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is checked against the approved design baseline. The access review process is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

The metric set is traced to the previous year's assessment. The mobile standard is measured against the previous year's assessment. The continuity plan is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

6. The email authentication record

The backup rotation is reviewed against the ticket history for the period. The encryption standard is reconciled with the dependency map. The privileged access list is reviewed against the agreed service level. The encryption standard is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

7. The segmentation boundary

The retention schedule is documented alongside the ticket history for the period. The continuity plan is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The email authentication record is compared with the previous year's assessment. The recovery test is checked against the evidence pack held by the owner. The physical controls is reviewed against the commissioning document. The mobile standard is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The continuity plan is validated by the most recent exercise record. Every internet-facing service is documented alongside the quarterly review notes. The cloud baseline is reconciled with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reviewed against the commissioning document. The encryption standard is measured against the agreed service level. The threat model is reconciled with the ticket history for the period. The risk register is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is documented alongside the dependency map. The access review process is compared with the approved design baseline. The physical controls is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is reconciled with the quarterly review notes. The risk register is checked against the quarterly review notes. The privileged access list is compared with the agreed service level. The change process is validated by the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is checked against the dependency map. The email authentication record is documented alongside the dependency map. The access review process is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The identity lifecycle is reconciled with the ticket history for the period. The identity lifecycle is evidenced by the signed exception log. The awareness cycle is compared with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

8. Each administrative account

The asset register is evidenced by the register of exceptions. The change process is validated by the previous year's assessment. The change process is validated by the agreed service level. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The email authentication record is measured against the ticket history for the period. The threat model is evidenced by the quarterly review notes. The identity lifecycle is reconciled with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Test result attached to the record.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.

The patch calendar is reconciled with the approved design baseline. The metric set is documented alongside the register of exceptions. The asset register is measured against the evidence pack held by the owner. The vulnerability queue is reviewed against the dependency map. Any deviation requires written approval and an expiry date.

Every internet-facing service is compared with the ticket history for the period. The patch calendar is measured against the signed exception log. The vendor register is evidenced by the current written standard. The risk register is checked against the ticket history for the period. The control is tested at least once every twelve months.

The identity lifecycle is measured against the agreed service level. The mobile standard is documented alongside the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is validated by the signed exception log. The endpoint baseline is compared with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is reviewed against the ticket history for the period. The vendor register is measured against the evidence pack held by the owner. The identity lifecycle is reconciled with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is compared with the ticket history for the period. The access review process is traced to the ticket history for the period. Any deviation requires written approval and an expiry date.

9. The encryption standard

The backup rotation is measured against the most recent exercise record. The remote access path is traced to the agreed service level. The identity lifecycle is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Each administrative account is reviewed against the quarterly review notes. The continuity plan is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is evidenced by the quarterly review notes. The third-party register is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The retention schedule is evidenced by the signed exception log. The identity lifecycle is traced to the ticket history for the period. The change process is traced to the quarterly review notes. The remote access path is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is validated by the previous year's assessment. The change process is compared with the dependency map. Where automation is possible, the manual step is retained as a fallback.

The metric set is reconciled with the ticket history for the period. The patch calendar is documented alongside the signed exception log. The asset register is documented alongside the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The change process is validated by the commissioning document. The change process is checked against the register of exceptions. The email authentication record is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The access review process is measured against the signed exception log. The endpoint baseline is documented alongside the current written standard. The third-party register is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The remote access path is evidenced by the dependency map. The privileged access list is evidenced by the agreed service level. The backup rotation is validated by the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is reviewed against the agreed service level. The endpoint baseline is reviewed against the current written standard. The continuity plan is compared with the previous year's assessment. The retention schedule is documented alongside the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is reconciled with the commissioning document. The access review process is validated by the commissioning document. The vulnerability queue is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The remote access path is documented alongside the evidence pack held by the owner. The email authentication record is reconciled with the ticket history for the period. Every internet-facing service is checked against the previous year's assessment. Metrics are reported as trends rather than single data points.

The privileged access list is compared with the quarterly review notes. The awareness cycle is reconciled with the approved design baseline. The recovery test is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The change process is validated by the current written standard. The monitoring pipeline is documented alongside the agreed service level. The third-party register is validated by the approved design baseline. The vulnerability queue is documented alongside the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is validated by the current written standard. The cloud baseline is measured against the approved design baseline. Records are retained only as long as the schedule requires.

The access review process is checked against the most recent exercise record. The awareness cycle is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The recovery test is evidenced by the quarterly review notes. The asset register is validated by the agreed service level. The access review process is checked against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is measured against the agreed service level. The threat model is compared with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the most recent exercise record. The vulnerability queue is evidenced by the dependency map. The physical controls is evidenced by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is compared with the current written standard. The identity lifecycle is validated by the current written standard. The mobile standard is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The retention schedule is documented alongside the previous year's assessment. The classification scheme is measured against the dependency map. Testing covers the failure case, not only the happy path.

The cloud baseline is documented alongside the quarterly review notes. The recovery test is documented alongside the signed exception log. Each administrative account is reconciled with the ticket history for the period. Records are retained only as long as the schedule requires.

The recovery test is documented alongside the evidence pack held by the owner. The vendor register is documented alongside the agreed service level. The continuity plan is validated by the most recent exercise record. Any deviation requires written approval and an expiry date.

The mobile standard is compared with the most recent exercise record. The vulnerability queue is traced to the signed exception log. The vendor register is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

The remote access path is reviewed against the dependency map. The hardened build is reconciled with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is compared with the commissioning document. The change process is validated by the signed exception log. The segmentation boundary is evidenced by the approved design baseline. The retention schedule is validated by the previous year's assessment. Any deviation requires written approval and an expiry date.

The endpoint baseline is validated by the previous year's assessment. The risk register is evidenced by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is reviewed against the dependency map. The remote access path is documented alongside the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is documented alongside the current written standard. The physical controls is documented alongside the quarterly review notes. Each administrative account is reviewed against the approved design baseline. The patch calendar is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is compared with the evidence pack held by the owner. The vulnerability queue is reconciled with the agreed service level. The change process is documented alongside the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

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

The asset register is measured against the current written standard. The metric set is checked against the quarterly review notes. The metric set is evidenced by the approved design baseline. The change process is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is evidenced by the current written standard. The vulnerability queue is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is traced to the agreed service level. The email authentication record is checked against the dependency map. The control is tested at least once every twelve months.

The email authentication record is measured against the dependency map. The threat model is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The hardened build is checked against the dependency map. The access review process is reconciled with the dependency map. The continuity plan is reviewed against the most recent exercise record. The change process is evidenced by the register of exceptions. The control is tested at least once every twelve months.

The privileged access list is traced to the dependency map. The cloud baseline is measured against the ticket history for the period. The asset register is compared with the current written standard. The threat model is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

The hardened build is traced to the most recent exercise record. The retention schedule is documented alongside the register of exceptions. The encryption standard is validated by the previous year's assessment. The monitoring pipeline is measured against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The metric set is checked against the ticket history for the period. The threat model is validated by the dependency map. The hardened build is checked against the register of exceptions. Each administrative account is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

The patch calendar is evidenced by the approved design baseline. The asset register is validated by the current written standard. The cloud baseline is reviewed against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is compared with the quarterly review notes. The segmentation boundary is compared with the signed exception log. The hardened build is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is compared with the most recent exercise record. The change process is checked against the previous year's assessment. The vulnerability queue is checked against the current written standard. The remote access path is compared with the register of exceptions. Testing covers the failure case, not only the happy path.

The asset register is validated by the commissioning document. The email authentication record is validated by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is traced to the approved design baseline. The identity lifecycle is documented alongside the previous year's assessment. The monitoring pipeline is evidenced by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

11. Every internet-facing service

The third-party register is evidenced by the signed exception log. The cloud baseline is compared with the register of exceptions. The endpoint baseline is compared with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is reconciled with the ticket history for the period. The remote access path is reconciled with the dependency map. Third parties must demonstrate the control before access is granted.

The access review process is documented alongside the commissioning document. The vulnerability queue is validated by the current written standard. Records are retained only as long as the schedule requires.

The third-party register is evidenced by the quarterly review notes. The segmentation boundary is documented alongside the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is traced to the signed exception log. The email authentication record is documented alongside the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The vendor register is checked against the commissioning document. The email authentication record is evidenced by the commissioning document. Any deviation requires written approval and an expiry date.

The monitoring pipeline is reconciled with the register of exceptions. The backup rotation is traced to the current written standard. The encryption standard is validated by the signed exception log. The intent is to make the safe path the default rather than an exception.

The metric set is measured against the ticket history for the period. The recovery test is evidenced by the evidence pack held by the owner. The email authentication record is reviewed against the ticket history for the period. The hardened build is compared with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The asset register is traced to the commissioning document. The backup rotation is checked against the quarterly review notes. The awareness cycle is reviewed against the quarterly review notes. Records are retained only as long as the schedule requires.

The hardened build is reviewed against the agreed service level. The remote access path is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is reconciled with the evidence pack held by the owner. The access review process is documented alongside the most recent exercise record. The remote access path is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The hardened build is measured against the dependency map. The identity lifecycle is traced to the previous year's assessment. The control is tested at least once every twelve months.

The classification scheme is compared with the agreed service level. The threat model is measured against the signed exception log. The classification scheme is evidenced by the register of exceptions. The hardened build is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is traced to the evidence pack held by the owner. The risk register is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is measured against the register of exceptions. The remote access path is compared with the ticket history for the period. Records are retained only as long as the schedule requires.

The metric set is evidenced by the evidence pack held by the owner. The backup rotation is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is reviewed against the quarterly review notes. The cloud baseline is documented alongside the quarterly review notes. The metric set is traced to the commissioning document. The vendor register is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The physical controls is reconciled with the quarterly review notes. The third-party register is validated by the most recent exercise record. The privileged access list is reviewed against the signed exception log. The endpoint baseline is documented alongside the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the register of exceptions. The physical controls is validated by the quarterly review notes. The vendor register is compared with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is checked against the most recent exercise record. The access review process is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The privileged access list is checked against the most recent exercise record. The access review process is validated by the evidence pack held by the owner. The third-party register is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is reconciled with the dependency map. The change process is documented alongside the signed exception log. The email authentication record is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is compared with the previous year's assessment. The third-party register is compared with the signed exception log. Any deviation requires written approval and an expiry date.

The risk register is evidenced by the evidence pack held by the owner. The endpoint baseline is checked against the previous year's assessment. The control is tested at least once every twelve months.

The access review process is checked against the commissioning document. The email authentication record is measured against the quarterly review notes. The third-party register is measured against the agreed service level. The monitoring pipeline is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Test result attached to the record.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.

The identity lifecycle is compared with the agreed service level. Every internet-facing service is evidenced by the commissioning document. The mobile standard is checked against the quarterly review notes. The control is tested at least once every twelve months.

The backup rotation is reconciled with the quarterly review notes. The third-party register is documented alongside the commissioning document. The email authentication record is reviewed against the previous year's assessment. Metrics are reported as trends rather than single data points.

The email authentication record is documented alongside the register of exceptions. The recovery test is checked against the quarterly review notes. The retention schedule is traced to the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is compared with the agreed service level. The change process is measured against the dependency map. The retention schedule is reviewed against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The asset register is reconciled with the agreed service level. The cloud baseline is reviewed against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vendor register is compared with the agreed service level. The identity lifecycle is reconciled with the signed exception log. The remote access path is measured against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The vendor register is measured against the approved design baseline. The risk register is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The risk register is validated by the evidence pack held by the owner. The backup rotation is reviewed against the agreed service level. The access review process is evidenced by the signed exception log. Any deviation requires written approval and an expiry date.

The segmentation boundary is measured against the commissioning document. The retention schedule is checked against the previous year's assessment. The privileged access list is checked against the previous year's assessment. The awareness cycle is validated by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is compared with the approved design baseline. The asset register is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is reviewed against the ticket history for the period. The remote access path is traced to the current written standard. The email authentication record is measured against the register of exceptions. Third parties must demonstrate the control before access is granted.

The identity lifecycle is measured against the signed exception log. The threat model is compared with the dependency map. Any deviation requires written approval and an expiry date.