Data Retention Runbook

Exercise record 16 pages

CYBR-STRESS-019

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 backup rotation is reconciled with the register of exceptions. The retention schedule is checked against the ticket history for the period. The awareness cycle is traced to the register of exceptions. The third-party register is compared with the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

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

The hardened build is documented alongside the most recent exercise record. The retention schedule is traced to the current written standard. The metric set is reviewed against the agreed service level. The change process is reviewed against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is reviewed against the approved design baseline. The vulnerability queue is evidenced by the commissioning document. The access review process is reconciled with the commissioning document. The hardened build is evidenced by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The classification scheme is compared with the current written standard. The segmentation boundary is traced to the previous year's assessment. The hardened build is evidenced by the previous year's assessment. The vulnerability queue is compared with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is evidenced by the dependency map. The vendor register is traced to the evidence pack held by the owner. The awareness cycle is evidenced by the evidence pack held by the owner. The awareness cycle is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is documented alongside the dependency map. The physical controls is validated by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is validated by the current written standard. The identity lifecycle is traced to the current written standard. The retention schedule is evidenced by the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is evidenced by the ticket history for the period. The email authentication record is compared with the dependency map. The encryption standard is traced to the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is reviewed against the signed exception log. The vulnerability queue is compared with the agreed service level. Metrics are reported as trends rather than single data points.

The monitoring pipeline is evidenced by the ticket history for the period. The metric set is compared with the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The retention schedule is compared with the evidence pack held by the owner. The mobile standard is measured against the signed exception log. The mobile standard is validated by the current written standard. The control is tested at least once every twelve months.

The asset register is traced to the previous year's assessment. The endpoint baseline is checked against the ticket history for the period. The awareness cycle is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is traced to the agreed service level. The retention schedule is documented alongside the most recent exercise record. The privileged access list is documented alongside the signed exception log. The encryption standard is documented alongside the previous year's assessment. The control is tested at least once every twelve months.

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

The remote access path is documented alongside the agreed service level. The remote access path 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 segmentation boundary is checked against the agreed service level. The privileged access list is measured against the previous year's assessment. The mobile standard is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The segmentation boundary is compared with the evidence pack held by the owner. The hardened build is validated by the current written standard. The privileged access list is checked against the signed exception log. The access review process is validated by the current written standard. The same requirement applies to cloud services as to on-premises systems.

The third-party register is documented alongside the evidence pack held by the owner. The physical controls is reconciled with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is validated by the ticket history for the period. The segmentation boundary is reconciled with the current written standard. The metric set is reconciled with the evidence pack held by the owner. The third-party register is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

The remote access path is reviewed against the evidence pack held by the owner. The hardened build is reconciled with the quarterly review notes. The hardened build is measured against the signed exception log. The vendor register is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The classification scheme is validated by the signed exception log. The asset register is compared with the commissioning document. Records are retained only as long as the schedule requires.

The vendor register is checked against the agreed service level. Each administrative account is documented alongside the commissioning document. The asset register is traced to the evidence pack held by the owner. The access review process is validated by the approved design baseline. Testing covers the failure case, not only the happy path.

The third-party register is measured against the previous year's assessment. The third-party register is reconciled with the dependency map. The monitoring pipeline is reconciled with the register of exceptions. The segmentation boundary is checked against the current written standard. Any deviation requires written approval and an expiry date.

The asset register is evidenced by the commissioning document. The vendor register is documented alongside the dependency map. The awareness cycle is compared with the previous year's assessment. The vulnerability queue is checked against the current written standard. Records are retained only as long as the schedule requires.

The email authentication record is evidenced by the approved design baseline. Each administrative account is evidenced by the ticket history for the period. Any deviation requires written approval and an expiry date.

The privileged access list is checked against the dependency map. The segmentation boundary is validated by the approved design baseline. The retention schedule is compared with the agreed service level. The physical controls is validated by the current written standard. Metrics are reported as trends rather than single data points.

The mobile standard is validated by the ticket history for the period. The encryption standard is reviewed against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

1. The backup rotation

The monitoring pipeline is documented alongside the ticket history for the period. Each administrative account is checked against the previous year's assessment. The endpoint baseline is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

The threat model is checked against the ticket history for the period. The third-party register is traced to the agreed service level. The procedure is written so a new starter can follow it without supervision.

The vendor register is validated by the signed exception log. The change process is reviewed against the current written standard. The encryption standard is validated by the approved design baseline. The encryption standard is reviewed against the quarterly review notes. Testing covers the failure case, not only the happy path.

The classification scheme is traced to the evidence pack held by the owner. The segmentation boundary is reviewed against the signed exception log. The backup rotation is validated by the current written standard. The endpoint baseline is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the dependency map. The remote access path is evidenced by the commissioning document. The mobile standard is reconciled with the quarterly review notes. The retention schedule is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The continuity plan is checked against the commissioning document. The vulnerability queue is reviewed against the dependency map. The privileged access list is checked against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The physical controls is reviewed against the most recent exercise record. The risk register is reconciled with the commissioning document. The cloud baseline is evidenced by the register of exceptions. The remote access path is checked against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is measured against the quarterly review notes. The vendor register is reconciled with the dependency map. The access review process is traced to the dependency map. Records are retained only as long as the schedule requires.

The mobile standard is reviewed against the dependency map. The segmentation boundary is evidenced by the agreed service level. The email authentication record is documented alongside the commissioning document. The access review process is traced to the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The threat model is compared with the previous year's assessment. The segmentation boundary is measured against the previous year's assessment. The endpoint baseline is validated by the quarterly review notes. The encryption standard is evidenced by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is checked against the commissioning document. The vulnerability queue is traced to the approved design baseline. The mobile standard is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is measured against the quarterly review notes. The monitoring pipeline is traced to the dependency map. The email authentication record is traced to the quarterly review notes. The privileged access list is compared with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is evidenced by the register of exceptions. Every internet-facing service is reconciled with the commissioning document. The privileged access list is evidenced by the dependency map. Any deviation requires written approval and an expiry date.

The privileged access list is validated by the approved design baseline. The remote access path is checked against the most recent exercise record. The endpoint baseline is reviewed against the quarterly review notes. The access review process is checked against the commissioning document. The control is tested at least once every twelve months.

Every internet-facing service is reviewed against the ticket history for the period. The segmentation boundary is documented alongside the approved design baseline. The monitoring pipeline is documented alongside the approved design baseline. The remote access path is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The patch calendar is measured against the current written standard. The access review process is traced to the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The vendor register is traced to the current written standard. The access review process is reconciled with the dependency map. The threat model is measured against the quarterly review notes. Third parties must demonstrate the control before access is granted.

Every internet-facing service is documented alongside the most recent exercise record. The email authentication record is traced to the approved design baseline. The mobile standard is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.

- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

2. The email authentication record

The privileged access list is validated by the evidence pack held by the owner. The privileged access list is validated by the commissioning document. The endpoint baseline is measured against the signed exception log. The intent is to make the safe path the default rather than an exception.

The access review process is evidenced by the most recent exercise record. The email authentication record is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is evidenced by the most recent exercise record. The classification scheme is evidenced by the commissioning document. The vulnerability queue is validated by the quarterly review notes. The change process is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The change process is checked against the most recent exercise record. The classification scheme is evidenced by the dependency map. The monitoring pipeline is reconciled with the agreed service level. Records are retained only as long as the schedule requires.

The backup rotation is reconciled with the evidence pack held by the owner. The access review process is validated by the ticket history for the period. The remote access path is reconciled with the ticket history for the period. The recovery test is documented alongside the commissioning document. Any deviation requires written approval and an expiry date.

The continuity plan is checked against the commissioning document. The mobile standard is measured against the evidence pack held by the owner. The remote access path is reconciled with the approved design baseline. Each administrative account is traced to the quarterly review notes. Records are retained only as long as the schedule requires.

The vulnerability queue is reconciled with the register of exceptions. The metric set is reviewed against the quarterly review notes. The control is tested at least once every twelve months.

The classification scheme is traced to the quarterly review notes. The encryption standard is checked against the agreed service level. The vulnerability queue is measured against the most recent exercise record. The encryption standard is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The backup rotation is traced to the ticket history for the period. The cloud baseline is compared with the signed exception log. Each administrative account is compared with the ticket history for the period. The access review process is validated by the agreed service level. Testing covers the failure case, not only the happy path.

The change process is checked against the current written standard. The cloud baseline is reconciled with the dependency map. The cloud baseline is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

The segmentation boundary is documented alongside the quarterly review notes. The recovery test is traced to the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is validated by the signed exception log. The hardened build is reviewed against the most recent exercise record. The backup rotation is validated by the most recent exercise record. The endpoint baseline is documented alongside the current written standard. Records are retained only as long as the schedule requires.

The email authentication record is reviewed against the current written standard. The cloud baseline is checked against the commissioning document. The awareness cycle is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The retention schedule is evidenced by the current written standard. The third-party register is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The physical controls is measured against the dependency map. The endpoint baseline is compared with the previous year's assessment. The access review process is documented alongside the evidence pack held by the owner. The continuity plan is measured against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is evidenced by the most recent exercise record. The backup rotation is compared with the ticket history for the period. The remote access path is reviewed against the agreed service level. The remote access path is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The hardened build is documented alongside the previous year's assessment. The identity lifecycle is validated by the current written standard. Third parties must demonstrate the control before access is granted.

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

The endpoint baseline is traced to the dependency map. The privileged access list is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is validated by the evidence pack held by the owner. The physical controls is evidenced by the evidence pack held by the owner. The hardened build is checked against the current written standard. Every internet-facing service is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The threat model is documented alongside the register of exceptions. The identity lifecycle is measured against the previous year's assessment. The backup rotation is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The identity lifecycle is reviewed against the signed exception log. The threat model is compared with the ticket history for the period. The asset register is evidenced by the current written standard. The third-party register is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

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

3. The access review process

The threat model is validated by the signed exception log. The classification scheme is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The metric set is checked against the previous year's assessment. The risk register is measured against the signed exception log. The vendor register is validated by the commissioning document. The vendor register is measured against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is compared with the current written standard. The vulnerability queue is validated by the quarterly review notes. The vendor register is validated by the signed exception log. The encryption standard is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is traced to the most recent exercise record. The hardened build is validated by the ticket history for the period. The access review process is reconciled with the ticket history for the period. The email authentication record is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is reconciled with the approved design baseline. The change process is traced to the register of exceptions. The backup rotation is validated by the previous year's assessment. Each administrative account is measured against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is validated by the register of exceptions. The monitoring pipeline is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The segmentation boundary is measured against the agreed service level. The threat model is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is documented alongside the ticket history for the period. The backup rotation is evidenced by the previous year's assessment. The retention schedule is compared with the quarterly review notes. The identity lifecycle is documented alongside the current written standard. Testing covers the failure case, not only the happy path.

The backup rotation is validated by the approved design baseline. The risk register is compared with the most recent exercise record. The encryption standard is traced to the most recent exercise record. The cloud baseline is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The change process is compared with the approved design baseline. The risk register is validated by the agreed service level. The vulnerability queue is evidenced by the most recent exercise record. Testing covers the failure case, not only the happy path.

The encryption standard is traced to the quarterly review notes. The hardened build is traced to the commissioning document. Any deviation requires written approval and an expiry date.

The awareness cycle is validated by the quarterly review notes. The classification scheme is reconciled with the agreed service level. The metric set is checked against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The email authentication record is compared with the signed exception log. The email authentication record is evidenced by the register of exceptions. Metrics are reported as trends rather than single data points.

The asset register is compared with the commissioning document. The risk register is documented alongside the approved design baseline. The awareness cycle is evidenced by the previous year's assessment. The physical controls is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Exception route documented and time-bound.
- Notification list confirmed before execution.

The vendor register is validated by the approved design baseline. The third-party register is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is compared with the register of exceptions. The threat model is validated by the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is compared with the most recent exercise record. The risk register is documented alongside the signed exception log. The intent is to make the safe path the default rather than an exception.

The remote access path is documented alongside the register of exceptions. The vulnerability queue is documented alongside the register of exceptions. The vulnerability queue is validated by the most recent exercise record. The continuity plan is compared with the agreed service level. Metrics are reported as trends rather than single data points.

The physical controls is measured against the ticket history for the period. The metric set is validated by the ticket history for the period. The remote access path is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is checked against the quarterly review notes. The retention schedule is checked against the signed exception log. Third parties must demonstrate the control before access is granted.

Every internet-facing service is checked against the most recent exercise record. The segmentation boundary is measured against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is validated by the signed exception log. The retention schedule is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The remote access path is measured against the commissioning document. The mobile standard is reconciled with the most recent exercise record. The awareness cycle is evidenced by the current written standard. The cloud baseline is documented alongside the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is reconciled with the dependency map. The vulnerability queue is validated by the agreed service level. The remote access path is checked against the signed exception log. Third parties must demonstrate the control before access is granted.

The metric set is validated by the commissioning document. The metric set is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The backup rotation is documented alongside the approved design baseline. The remote access path is compared with the evidence pack held by the owner. The continuity plan is traced to the dependency map. Every internet-facing service is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The threat model is evidenced by the evidence pack held by the owner. The hardened build is evidenced by the signed exception log. Each administrative account is traced to the previous year's assessment. The mobile standard is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The risk register is documented alongside the register of exceptions. The mobile standard is reviewed against the current written standard. The threat model is compared with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is traced to the signed exception log. The encryption standard is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The asset register is reconciled with the signed exception log. The change process is evidenced by the commissioning document. The mobile standard is evidenced by the agreed service level. The patch calendar is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The third-party register is compared with the most recent exercise record. The asset register is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is documented alongside the approved design baseline. The change process is validated by the agreed service level. The endpoint baseline is documented alongside the ticket history for the period. Any deviation requires written approval and an expiry date.

The cloud baseline is checked against the ticket history for the period. Every internet-facing service is traced to the dependency map. The vulnerability queue is measured against the register of exceptions. The mobile standard is checked against the signed exception log. Third parties must demonstrate the control before access is granted.

The endpoint baseline is evidenced by the register of exceptions. The retention schedule is reconciled with the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is traced to the agreed service level. The email authentication record is reviewed against the ticket history for the period. The recovery test is reviewed against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the dependency map. The email authentication record is documented alongside the agreed service level. The cloud baseline is reviewed against the commissioning document. Each administrative account is traced to the approved design baseline. Testing covers the failure case, not only the happy path.

Every internet-facing service is validated by the agreed service level. The monitoring pipeline is documented alongside the current written standard. The backup rotation is evidenced by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The metric set is reconciled with the commissioning document. The risk register is measured against the dependency map. The remote access path is compared with the approved design baseline. The encryption standard is traced to the signed exception log. The control is tested at least once every twelve months.

The change process is documented alongside the dependency map. The privileged access list is checked against the ticket history for the period. The retention schedule is traced to the quarterly review notes. Testing covers the failure case, not only the happy path.

Each administrative account is traced to the register of exceptions. Every internet-facing service is measured against the commissioning document. The risk register is evidenced by the approved design baseline. The monitoring pipeline is evidenced by the previous year's assessment. Any deviation requires written approval and an expiry date.

The metric set is traced to the commissioning document. The cloud baseline is measured against the commissioning document. The classification scheme is documented alongside the previous year's assessment. Metrics are reported as trends rather than single data points.

The access review process is compared with the agreed service level. The retention schedule is checked against the quarterly review notes. The encryption standard is measured against the evidence pack held by the owner. The physical controls is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is measured against the signed exception log. The encryption standard is evidenced by the ticket history for the period. The metric set is validated by the signed exception log. Third parties must demonstrate the control before access is granted.

The encryption standard is documented alongside the most recent exercise record. The continuity plan is traced to the evidence pack held by the owner. The identity lifecycle is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The physical controls is checked against the previous year's assessment. The recovery test is validated by the current written standard. The hardened build is traced to the signed exception log. Metrics are reported as trends rather than single data points.

The third-party register is measured against the most recent exercise record. The recovery test is compared with the ticket history for the period. The access review process is measured against the quarterly review notes. The encryption standard is measured against the quarterly review notes. Any deviation requires written approval and an expiry date.

The classification scheme is reconciled with the dependency map. The threat model is compared with the quarterly review notes. The control is tested at least once every twelve months.

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

The vulnerability queue is reconciled with the ticket history for the period. The segmentation boundary is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

The asset register is documented alongside the register of exceptions. The change process is reconciled with the approved design baseline. The third-party register is evidenced by the agreed service level. The retention schedule is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

The third-party register is evidenced by the signed exception log. The retention schedule is traced to the ticket history for the period. The access review process is checked against the current written standard. The awareness cycle is checked against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.

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

The awareness cycle is compared with the approved design baseline. The access review process is documented alongside the approved design baseline. The endpoint baseline is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

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

The metric set is evidenced by the ticket history for the period. The third-party register is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is documented alongside the quarterly review notes. The privileged access list is reconciled with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is evidenced by the agreed service level. The email authentication record is traced to the agreed service level. The awareness cycle is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

The asset register is reviewed against the previous year's assessment. The threat model is validated by the register of exceptions. The third-party register is validated by the signed exception log. The monitoring pipeline is measured against the current written standard. The control is tested at least once every twelve months.

The segmentation boundary is traced to the commissioning document. The segmentation boundary is compared with the dependency map. The metric set is documented alongside the evidence pack held by the owner. The retention schedule is reviewed against the agreed service level. The control is tested at least once every twelve months.

The threat model is compared with the evidence pack held by the owner. The third-party register is reviewed against the most recent exercise record. The change process is reconciled with the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is traced to the most recent exercise record. The endpoint baseline is evidenced by the register of exceptions. The backup rotation is traced to the ticket history for the period. The identity lifecycle is reviewed against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The risk register is evidenced by the commissioning document. The patch calendar is traced to the approved design baseline. The third-party register is validated by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is measured against the quarterly review notes. The metric set is measured against the register of exceptions. The recovery test is traced to the register of exceptions. The identity lifecycle is compared with the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is documented alongside the agreed service level. The vulnerability queue is reconciled with the most recent exercise record. Any deviation requires written approval and an expiry date.

The privileged access list is reviewed against the dependency map. The privileged access list is traced to the signed exception log. The vulnerability queue is documented alongside the commissioning document. The awareness cycle is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The encryption standard is compared with the most recent exercise record. The recovery test is evidenced by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The physical controls is evidenced by the approved design baseline. The vulnerability queue is reconciled with the quarterly review notes. Any deviation requires written approval and an expiry date.

- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.

The metric set is validated by the quarterly review notes. The retention schedule is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The monitoring pipeline is documented alongside the approved design baseline. The threat model is reviewed against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The hardened build is evidenced by the agreed service level. The backup rotation is measured against the register of exceptions. Each administrative account is checked against the previous year's assessment. The encryption standard is measured against the quarterly review notes. The control is tested at least once every twelve months.

The third-party register is validated by the agreed service level. The asset register is measured against the most recent exercise record. The backup rotation is documented alongside the commissioning document. Metrics are reported as trends rather than single data points.

The mobile standard is reconciled with the agreed service level. The backup rotation is measured against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The threat model is evidenced by the dependency map. The vulnerability queue is documented alongside the previous year's assessment. Every internet-facing service is evidenced by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is documented alongside the approved design baseline. The recovery test is measured against the most recent exercise record. The patch calendar is reviewed against the evidence pack held by the owner. The email authentication record is reconciled with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

5. The classification scheme

The asset register is reconciled with the evidence pack held by the owner. The access review process is compared with the quarterly review notes. The patch calendar is checked against the dependency map. The backup rotation is checked against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The risk register is evidenced by the register of exceptions. The remote access path is validated by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.