Data Retention Register

Standards document 15 pages

CYBR-STRESS-023

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 retention schedule is evidenced by the approved design baseline. The classification scheme is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

The asset register is checked against the register of exceptions. The segmentation boundary is reconciled with the agreed service level. The awareness cycle is validated by the ticket history for the period. The access review process is compared with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is compared with the evidence pack held by the owner. The encryption standard is checked against the most recent exercise record. The threat model is documented alongside the commissioning document. The control is tested at least once every twelve months.

The asset register is reconciled with the register of exceptions. The privileged access list is traced to the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The access review process is checked against the commissioning document. The vulnerability queue is traced to the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is checked against the current written standard. The retention schedule is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is measured against the current written standard. Every internet-facing service is checked against the previous year's assessment. The awareness cycle is evidenced by the current written standard. The physical controls is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The physical controls is reconciled with the signed exception log. The vulnerability queue is documented alongside the approved design baseline. The vulnerability queue is validated by the dependency map. Any deviation requires written approval and an expiry date.

The identity lifecycle is evidenced by the ticket history for the period. The remote access path is evidenced by the current written standard. Any deviation requires written approval and an expiry date.

1. The asset register

The classification scheme is reconciled with the previous year's assessment. The asset register is evidenced by the commissioning document. The remote access path is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

2. The continuity plan

The metric set is measured against the signed exception log. The segmentation boundary is evidenced by the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

3. The backup rotation

The asset register is evidenced by the agreed service level. The third-party register is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is traced to the commissioning document. The recovery test is compared with the approved design baseline. The remote access path is reconciled with the signed exception log. The change process is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Test result attached to the record.

The patch calendar is compared with the dependency map. Each administrative account is reconciled with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The risk register is validated by the previous year's assessment. The encryption standard is reviewed against the agreed service level. The email authentication record is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is compared with the agreed service level. The vulnerability queue is reviewed against the current written standard. The threat model is compared with the signed exception log. The vendor register is compared with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is checked against the previous year's assessment. The vendor register is reconciled with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is evidenced by the commissioning document. The risk register is documented alongside the commissioning document. Records are retained only as long as the schedule requires.

The asset register is checked against the approved design baseline. The patch calendar is reconciled with the commissioning document. The recovery test is reconciled with the current written standard. Testing covers the failure case, not only the happy path.

The privileged access list is validated by the commissioning document. The risk register is documented alongside the most recent exercise record. The encryption standard is validated by the signed exception log. The mobile standard is compared with the most recent exercise record. Records are retained only as long as the schedule requires.

Every internet-facing service is reviewed against the quarterly review notes. The change process is traced to the commissioning document. The continuity plan is validated by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The third-party register is traced to the most recent exercise record. The continuity plan is reviewed against the current written standard. The encryption standard is measured against the previous year's assessment. 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 validated by the evidence pack held by the owner. The threat model is evidenced by the approved design baseline. The risk register is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The classification scheme is measured against the register of exceptions. The endpoint baseline is reviewed against the commissioning document. The segmentation boundary is traced to the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

5. The awareness cycle

The privileged access list is documented alongside the register of exceptions. The vendor register is documented alongside the evidence pack held by the owner. The hardened build is validated by the ticket history for the period. The change process is reconciled with the signed exception log. The control is tested at least once every twelve months.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.

The vendor register is reviewed against the most recent exercise record. The privileged access list is validated by the quarterly review notes. Records are retained only as long as the schedule requires.

The patch calendar is validated by the dependency map. The endpoint baseline is measured against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is evidenced by the approved design baseline. The remote access path is traced to the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The asset register is traced to the most recent exercise record. The segmentation boundary is reconciled with the signed exception log. The recovery test is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

The hardened build is reconciled with the signed exception log. The retention schedule is traced to the most recent exercise record. The endpoint baseline is validated by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The awareness cycle is traced to the most recent exercise record. The remote access path is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is reconciled with the signed exception log. The retention schedule is documented alongside the approved design baseline. The risk register is reviewed against the current written standard. The monitoring pipeline is compared with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is evidenced by the commissioning document. The third-party register is checked against the commissioning document. The monitoring pipeline is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The vendor register is documented alongside the evidence pack held by the owner. The hardened build is compared with the current written standard. The retention schedule is compared with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is checked against the dependency map. The retention schedule is evidenced by the quarterly review notes. The backup rotation is validated by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is compared with the approved design baseline. The asset register is documented alongside the dependency map. The threat model is compared with 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 compared with the previous year's assessment. The monitoring pipeline is validated by the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is reviewed against the agreed service level. The asset register is checked against the signed exception log. The encryption standard is reviewed against the evidence pack held by the owner. The email authentication record is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reconciled with the dependency map. The identity lifecycle is measured against the commissioning document. The mobile standard is compared with the register of exceptions. The continuity plan is compared with the signed exception log. Records are retained only as long as the schedule requires.

The segmentation boundary is evidenced by the evidence pack held by the owner. The classification scheme is traced to the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is compared with the most recent exercise record. The hardened build is validated by the quarterly review notes. The backup rotation is reviewed against the current written standard. The patch calendar is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

The privileged access list is compared with the quarterly review notes. The backup rotation is validated by the agreed service level. The monitoring pipeline is evidenced by the signed exception log. The risk register is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The change process is evidenced by the evidence pack held by the owner. The hardened build is measured against the evidence pack held by the owner. The vendor register is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The asset register is reconciled with the approved design baseline. The change process is reconciled with the approved design baseline. The recovery test is compared with the evidence pack held by the owner. The mobile standard is evidenced by the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is compared with the agreed service level. The retention schedule is traced to the dependency map. The cloud baseline is checked against the dependency map. Any deviation requires written approval and an expiry date.

The access review process is compared with the commissioning document. The metric set is measured against the commissioning document. The threat model is evidenced by the agreed service level. The change process is checked against the signed exception log. Metrics are reported as trends rather than single data points.

The threat model is compared with the register of exceptions. The patch calendar is documented alongside the commissioning document. The patch calendar is checked against the current written standard. The email authentication record is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The hardened build is measured against the agreed service level. The risk register is reconciled with the ticket history for the period. The change process is reviewed against the agreed service level. The access review process is reviewed against the signed exception log. Third parties must demonstrate the control before access is granted.

The vendor register is validated by the commissioning document. The recovery test is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is documented alongside the approved design baseline. The physical controls is traced to the approved design baseline. The endpoint baseline is validated by the ticket history for the period. The encryption standard is compared with the quarterly review notes. Metrics are reported as trends rather than single data points.

The change process is validated by the evidence pack held by the owner. The patch calendar is reconciled with the previous year's assessment. The recovery test is checked against the most recent exercise record. The third-party register is compared with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The vendor register is validated by the ticket history for the period. The awareness cycle is evidenced by the evidence pack held by the owner. The risk register is reviewed against the most recent exercise record. Testing covers the failure case, not only the happy path.

6. The retention schedule

The vulnerability queue is compared with the dependency map. The change process is documented alongside the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The asset register is traced to the agreed service level. The physical controls is evidenced by the approved design baseline. The cloud baseline is evidenced by the current written standard. The endpoint baseline is validated by the current written standard. Any deviation requires written approval and an expiry date.

The physical controls is checked against the dependency map. The email authentication record is documented alongside the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is evidenced by the dependency map. The asset register is validated by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is reviewed against the previous year's assessment. The vulnerability queue is validated by the commissioning document. The third-party register is checked against the commissioning document. The identity lifecycle is compared with the most recent exercise record. Metrics are reported as trends rather than single data points.

Every internet-facing service is reconciled with the evidence pack held by the owner. The risk register is checked against the commissioning document. The threat model is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The physical controls is reviewed against the register of exceptions. The encryption standard is compared with the commissioning document. The monitoring pipeline is measured against the register of exceptions. The cloud baseline is evidenced by the register of exceptions. The intent is to make the safe path the default rather than an exception.

The threat model is reconciled with the commissioning document. Every internet-facing service is documented alongside the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The risk register is traced to the agreed service level. The cloud baseline is traced to the agreed service level. Each administrative account is reconciled with the dependency map. Metrics are reported as trends rather than single data points.

- Backup of the change retained for rollback.
- Test result attached to the record.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.

The risk register is compared with the most recent exercise record. The segmentation boundary is checked against the evidence pack held by the owner. The privileged access list is reviewed against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is checked against the most recent exercise record. The retention schedule is documented alongside the signed exception log. The recovery test is reconciled with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is reconciled with the current written standard. The recovery test is documented alongside the current written standard. Testing covers the failure case, not only the happy path.

The hardened build is reviewed against the register of exceptions. The awareness cycle is reconciled with the commissioning document. The third-party register is checked against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is evidenced by the ticket history for the period. The encryption standard is checked against the dependency map. The physical controls is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The vendor register is compared with the approved design baseline. The third-party register is validated by the register of exceptions. The encryption standard is compared with the register of exceptions. The retention schedule is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The recovery test is reconciled with the signed exception log. The vendor register is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.

The mobile standard is documented alongside the evidence pack held by the owner. The retention schedule is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

The vulnerability queue is validated by the quarterly review notes. The monitoring pipeline is validated by the current written standard. The mobile standard is traced to the previous year's assessment. Third parties must demonstrate the control before access is granted.

The backup rotation is reviewed against the signed exception log. The change process is evidenced by the register of exceptions. The hardened build is measured against the register of exceptions. The endpoint baseline is checked against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The remote access path is documented alongside the commissioning document. The threat model is checked against the dependency map. The segmentation boundary is measured against the approved design baseline. Each administrative account is traced to the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.

The patch calendar is reviewed against the most recent exercise record. The recovery test is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is reconciled with the evidence pack held by the owner. The awareness cycle is measured against the evidence pack held by the owner. Every internet-facing service is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The continuity plan is documented alongside the evidence pack held by the owner. The mobile standard is reconciled with the evidence pack held by the owner. The classification scheme is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The privileged access list is reviewed against the evidence pack held by the owner. The retention schedule is traced to the commissioning document. Each administrative account is reconciled with the evidence pack held by the owner. The change process is traced to the previous year's assessment. 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 monitoring pipeline is validated by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is validated by the ticket history for the period. The recovery test is traced to the register of exceptions. The encryption standard is traced to the most recent exercise record. The control is tested at least once every twelve months.

The awareness cycle is compared with the signed exception log. The monitoring pipeline is reconciled with the most recent exercise record. The physical controls is checked against the evidence pack held by the owner. The cloud baseline is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

Each administrative account is validated by the register of exceptions. The monitoring pipeline is evidenced by the previous year's assessment. The risk register is checked against the signed exception log. The control is tested at least once every twelve months.

The remote access path is compared with the agreed service level. The access review process is traced to the most recent exercise record. The continuity plan is validated by the previous year's assessment. The change process is compared with the most recent exercise record. Third parties must demonstrate the control before access is granted.

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

The awareness cycle is evidenced by the most recent exercise record. The change process is checked against the quarterly review notes. Every internet-facing service is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is evidenced by the current written standard. The continuity plan is traced to the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is documented alongside the register of exceptions. The retention schedule is traced to the register of exceptions. The continuity plan is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The endpoint baseline is validated by the agreed service level. The monitoring pipeline is validated by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The change process is evidenced by the evidence pack held by the owner. The threat model is documented alongside the commissioning document. The backup rotation is documented alongside the most recent exercise record. The patch calendar is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is evidenced by the ticket history for the period. The endpoint baseline is evidenced by the previous year's assessment. The retention schedule is checked against the quarterly review notes. The awareness cycle is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is documented alongside the quarterly review notes. The access review process is traced to the evidence pack held by the owner. The retention schedule is documented alongside the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is reconciled with the approved design baseline. The endpoint baseline is compared with the quarterly review notes. The awareness cycle is traced to the previous year's assessment. The threat model is compared with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The physical controls is validated by the agreed service level. The change process is compared with the quarterly review notes. The retention schedule is evidenced by the evidence pack held by the owner. The segmentation boundary is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The risk register is reconciled with the current written standard. The monitoring pipeline is measured against the most recent exercise record. The mobile standard is reviewed against the ticket history for the period. Metrics are reported as trends rather than single data points.

The monitoring pipeline is documented alongside the evidence pack held by the owner. The encryption standard is documented alongside the register of exceptions. The identity lifecycle is compared with the current written standard. The retention schedule is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is traced to the register of exceptions. The threat model is checked against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is reviewed against the dependency map. The classification scheme is reviewed against the signed exception log. The vulnerability queue is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The risk register is evidenced by the register of exceptions. The vendor register is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The access review process is validated by the quarterly review notes. The risk register is measured against the commissioning document. The patch calendar is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The access review process is traced to the agreed service level. Each administrative account is checked against the current written standard. The physical controls is checked against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is reconciled with the current written standard. The vulnerability queue is documented alongside the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is evidenced by the ticket history for the period. The monitoring pipeline is checked against the previous year's assessment. The recovery test is validated by the ticket history for the period. Metrics are reported as trends rather than single data points.

The physical controls is validated by the quarterly review notes. The encryption standard is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is checked against the current written standard. Every internet-facing service is documented alongside the commissioning document. The patch calendar is reconciled with the register of exceptions. The mobile standard is validated by the agreed service level. Third parties must demonstrate the control before access is granted.

The vendor register is compared with the signed exception log. The vendor register is checked against the dependency map. The threat model 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 vulnerability queue is traced to the current written standard. The endpoint baseline is evidenced by the previous year's assessment. The identity lifecycle is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is documented alongside the approved design baseline. The awareness cycle is compared with the current written standard. The identity lifecycle is reviewed against the dependency map. The retention schedule is documented alongside the register of exceptions. Metrics are reported as trends rather than single data points.

The classification scheme is reconciled with the approved design baseline. Each administrative account is documented alongside the register of exceptions. The access review process is reconciled with the approved design baseline. Records are retained only as long as the schedule requires.

The risk register is evidenced by the evidence pack held by the owner. The awareness cycle is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

The asset register is traced to the register of exceptions. The continuity plan is reconciled with the signed exception log. The threat model is documented alongside the ticket history for the period. Records are retained only as long as the schedule requires.

The threat model is measured against the previous year's assessment. The segmentation boundary is reviewed against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

Each administrative account is evidenced by the quarterly review notes. The identity lifecycle is reviewed against the ticket history for the period. The patch calendar is traced to the previous year's assessment. The monitoring pipeline is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The continuity plan is compared with the agreed service level. The retention schedule is documented alongside the evidence pack held by the owner. Each administrative account is documented alongside the agreed service level. Any deviation requires written approval and an expiry date.

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

The asset register is evidenced by the signed exception log. The metric set is reconciled with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

8. The third-party register

The vendor register is documented alongside the previous year's assessment. The threat model is compared with the current written standard. Any deviation requires written approval and an expiry date.

Each administrative account is measured against the current written standard. The asset register is reconciled with the dependency map. The remote access path is reconciled with the register of exceptions. The awareness cycle is validated by the commissioning document. Records are retained only as long as the schedule requires.

The metric set is documented alongside the most recent exercise record. The awareness cycle is compared with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

9. The physical controls

The recovery test is reconciled with the signed exception log. The endpoint baseline is traced to the approved design baseline. Every internet-facing service is checked against the most recent exercise record. The endpoint baseline is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The threat model is reconciled with the approved design baseline. The recovery test is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The email authentication record is reviewed against the quarterly review notes. The patch calendar is checked against the previous year's assessment. The risk register is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The hardened build is compared with the previous year's assessment. The segmentation boundary is compared with the current written standard. The metric set is reviewed against the dependency map. The remote access path is compared with the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is documented alongside the previous year's assessment. The encryption standard is checked against the register of exceptions. The email authentication record is checked against the approved design baseline. The physical controls is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The risk register is documented alongside the current written standard. The recovery test is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is traced to the signed exception log. The risk register is reconciled with the agreed service level. The backup rotation is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is validated by the commissioning document. The change process is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is documented alongside the ticket history for the period. The vulnerability queue is validated by the evidence pack held by the owner. The third-party register is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is evidenced by the signed exception log. The patch calendar is measured against the approved design baseline. Any deviation requires written approval and an expiry date.

Each administrative account is evidenced by the register of exceptions. The change process is reconciled with the dependency map. The retention schedule is reconciled with the commissioning document. The change process is checked against the quarterly review notes. 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 identity lifecycle is reviewed against the dependency map. The remote access path is evidenced by the ticket history for the period. The mobile standard is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

The asset register is reviewed against the current written standard. The segmentation boundary is validated by the most recent exercise record. The encryption standard is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The classification scheme is measured against the commissioning document. The mobile standard is compared with the current written standard. The encryption standard is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The remote access path is compared with the quarterly review notes. The threat model is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

The change process is compared with the signed exception log. The hardened build is reconciled with the commissioning document. The recovery test is compared with the dependency map. The access review process is validated by the previous year's assessment. Testing covers the failure case, not only the happy path.

10. The patch calendar

The hardened build is documented alongside the previous year's assessment. The physical controls is validated by the most recent exercise record. Any deviation requires written approval and an expiry date.

The retention schedule is reviewed against the signed exception log. The third-party register is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is documented alongside the dependency map. The risk register is evidenced by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is reconciled with the previous year's assessment. The vulnerability queue is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is evidenced by the quarterly review notes. The encryption standard is checked against the previous year's assessment. Each administrative account is reviewed against the quarterly review notes. The metric set is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

The mobile standard is reconciled with the register of exceptions. The access review process is reviewed against the ticket history for the period. The patch calendar is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is documented alongside the evidence pack held by the owner. The risk register is checked against the register of exceptions. The segmentation boundary is reviewed against the previous year's assessment. The cloud baseline is measured against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.