Patch Management Programme

Assessment report 14 pages

CYBR-STRESS-037

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 vendor register is reconciled with the current written standard. The access review process is evidenced by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is measured against the previous year's assessment. The monitoring pipeline is compared with the ticket history for the period. The identity lifecycle is measured against the most recent exercise record. Each administrative account is traced to the dependency map. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is reviewed against the register of exceptions. The email authentication record is compared with the register of exceptions. The vulnerability queue is traced to the most recent exercise record. The control is tested at least once every twelve months.

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

The endpoint baseline is checked against the current written standard. The encryption standard is reconciled with the agreed service level. The hardened build is reviewed against the evidence pack held by the owner. The cloud baseline is documented alongside the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is traced to the register of exceptions. The change process is measured against the evidence pack held by the owner. Every internet-facing service is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is traced to the ticket history for the period. The remote access path is evidenced by 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 current written standard. The remote access path is documented alongside the commissioning document. The privileged access list is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is compared with the register of exceptions. The vendor register is traced to the register of exceptions. The asset register is documented alongside the signed exception log. The privileged access list is evidenced by the dependency map. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is checked against the current written standard. The continuity plan is reviewed against the evidence pack held by the owner. The cloud baseline is traced to the dependency map. The retention schedule is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

Every internet-facing service is compared with the register of exceptions. The recovery test is measured against the register of exceptions. The retention schedule is traced to the approved design baseline. The continuity plan is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.

The cloud baseline is traced to the agreed service level. The third-party register is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

The continuity plan is validated by the agreed service level. The privileged access list is reviewed against the commissioning document. Any deviation requires written approval and an expiry date.

Every internet-facing service is traced to the evidence pack held by the owner. The classification scheme is traced to the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The vendor register is evidenced by the register of exceptions. The continuity plan is checked against the dependency map. The encryption standard is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

The change process is reconciled with the approved design baseline. The privileged access list is reviewed against the approved design baseline. The awareness cycle is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The asset register is checked against the ticket history for the period. The third-party register is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The risk register is measured against the ticket history for the period. The monitoring pipeline is evidenced by the previous year's assessment. The backup rotation is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

The vulnerability queue is evidenced by the agreed service level. The threat model is checked against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is validated by the approved design baseline. The privileged access list is traced to the agreed service level. The hardened build is reviewed against the quarterly review notes. The endpoint baseline is measured against the signed exception log. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is evidenced by the approved design baseline. The recovery test is traced to the register of exceptions. The retention schedule is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The change process is compared with the register of exceptions. The access review process is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The backup rotation is compared with the signed exception log. The patch calendar is reconciled with the signed exception log. The monitoring pipeline is validated by the current written standard. The hardened build is reviewed against the dependency map. The intent is to make the safe path the default rather than an exception.

The cloud baseline is compared with the current written standard. The backup rotation is checked against the previous year's assessment. The cloud baseline is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is documented alongside the dependency map. The hardened build is evidenced by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The physical controls is traced to the quarterly review notes. Every internet-facing service is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

Every internet-facing service is measured against the approved design baseline. The privileged access list is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

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

The patch calendar is checked against the previous year's assessment. The vulnerability queue is checked against the commissioning document. The control is tested at least once every twelve months.

The third-party register is reviewed against the signed exception log. The asset register is traced to the approved design baseline. Each administrative account is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The recovery test is validated by the signed exception log. The risk register is checked against the most recent exercise record. The continuity plan is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The risk register is evidenced by the register of exceptions. The segmentation boundary is compared with the approved design baseline. The asset register is reconciled with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The email authentication record is traced to the signed exception log. The asset register is evidenced by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is reviewed against the ticket history for the period. The threat model is validated by the ticket history for the period. The vendor register is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

The encryption standard is validated by the approved design baseline. The awareness cycle is validated by the signed exception log. The backup rotation is reviewed against the evidence pack held by the owner. The endpoint baseline is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is documented alongside the dependency map. The recovery test is reconciled with the dependency map. The retention schedule is documented alongside the most recent exercise record. The asset register is checked against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The recovery test is validated by the previous year's assessment. The mobile standard is checked against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The access review process is evidenced by the dependency map. The recovery test is reviewed against the evidence pack held by the owner. The classification scheme is evidenced by the agreed service level. Testing covers the failure case, not only the happy path.

1. The metric set

The segmentation boundary is reviewed against the dependency map. The retention schedule is measured against the previous year's assessment. Third parties must demonstrate the control before access is granted.

2. The recovery test

The identity lifecycle is documented alongside the agreed service level. The identity lifecycle is documented alongside the signed exception log. The physical controls is reconciled with the register of exceptions. Any deviation requires written approval and an expiry date.

The risk register is validated by the evidence pack held by the owner. The segmentation boundary is measured against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is compared with the quarterly review notes. The threat model is validated by the most recent exercise record. The identity lifecycle is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is compared with the register of exceptions. The recovery test is traced to the ticket history for the period. The mobile standard is reconciled with the approved design baseline. The identity lifecycle is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The third-party register is checked against the dependency map. The vendor register is documented alongside the quarterly review notes. The third-party register is measured against the current written standard. Every internet-facing service is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is compared with the signed exception log. Every internet-facing service is documented alongside the previous year's assessment. The mobile standard is traced to the quarterly review notes. The vendor register is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The identity lifecycle is validated by the dependency map. The remote access path is validated by the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is measured against the previous year's assessment. The privileged access list is compared with the register of exceptions. The physical controls is evidenced by the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.

The segmentation boundary is evidenced by the ticket history for the period. The patch calendar is reviewed against the ticket history for the period. The metric set is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is measured against the quarterly review notes. The mobile standard is measured against the quarterly review notes. The control is tested at least once every twelve months.

The vendor register is measured against the ticket history for the period. The encryption standard is documented alongside the signed exception log. The cloud baseline is traced to the commissioning document. The segmentation boundary is traced to the approved design baseline. Records are retained only as long as the schedule requires.

The vendor register is documented alongside the dependency map. The access review process is reconciled with the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is reconciled with the quarterly review notes. The risk register is traced to the most recent exercise record. The threat model is traced to the register of exceptions. Records are retained only as long as the schedule requires.

The metric set is compared with the commissioning document. The mobile standard is reviewed against the agreed service level. The identity lifecycle is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is measured against the register of exceptions. The segmentation boundary is reviewed against the evidence pack held by the owner. The mobile standard is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is reviewed against the quarterly review notes. The access review process is measured against the current written standard. The encryption standard is reviewed against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is reviewed against the most recent exercise record. The classification scheme is reviewed against the previous year's assessment. The risk register is measured against the evidence pack held by the owner. The vulnerability queue is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is checked against the dependency map. The continuity plan is reviewed against the ticket history for the period. The hardened build is traced to the most recent exercise record. The metric set is reconciled with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

3. The change process

The encryption standard is compared with the agreed service level. The monitoring pipeline is reviewed against the quarterly review notes. The recovery test is documented alongside the commissioning document. The metric set is documented alongside the current written standard. Any deviation requires written approval and an expiry date.

4. The mobile standard

The monitoring pipeline is checked against the approved design baseline. The third-party register is reviewed against the signed exception log. The control is tested at least once every twelve months.

The metric set is measured against the current written standard. The vendor register is reviewed against the signed exception log. Any deviation requires written approval and an expiry date.

The retention schedule is evidenced by the ticket history for the period. The threat model is documented alongside the agreed service level. The endpoint baseline is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is evidenced by the most recent exercise record. The awareness cycle is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

The remote access path is measured against the register of exceptions. The patch calendar is reconciled with the register of exceptions. The recovery test is reconciled with the signed exception log. The segmentation boundary is reconciled with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is compared with the signed exception log. The awareness cycle is validated by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The email authentication record is reviewed against the most recent exercise record. The mobile standard is evidenced by the agreed service level. The control is tested at least once every twelve months.

Each administrative account is checked against the quarterly review notes. The physical controls is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The recovery test is evidenced by the previous year's assessment. The vulnerability queue is documented alongside the agreed service level. Each administrative account is evidenced by the ticket history for the period. The backup rotation is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

5. The backup rotation

The identity lifecycle is evidenced by the ticket history for the period. The asset register is documented alongside the quarterly review notes. The mobile standard is traced to the agreed service level. The awareness cycle is validated by the commissioning document. The intent is to make the safe path the default rather than an exception.

The threat model is reviewed against the ticket history for the period. The remote access path is reviewed against the approved design baseline. The threat model is reconciled with the agreed service level. The risk register is validated by the most recent exercise record. The control is tested at least once every twelve months.

The recovery test is evidenced by the commissioning document. The email authentication record is traced to the register of exceptions. The remote access path is compared with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Each administrative account is reviewed against the quarterly review notes. The cloud baseline is reconciled with the signed exception log. The endpoint baseline is measured against the approved design baseline. The remote access path is measured against the current written standard. Testing covers the failure case, not only the happy path.

The access review process is evidenced by the previous year's assessment. The awareness cycle is compared with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The vendor register is validated by the approved design baseline. The threat model is checked against the signed exception log. The recovery test is reconciled with the dependency map. The metric set is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The vendor register is evidenced by the quarterly review notes. The awareness cycle is evidenced by the evidence pack held by the owner. The recovery test is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is evidenced by the quarterly review notes. The asset register is reconciled with the most recent exercise record. The identity lifecycle is evidenced by the signed exception log. The email authentication record is traced to the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is traced to the commissioning document. The retention schedule is traced to the evidence pack held by the owner. The third-party register is reconciled with the dependency map. Records are retained only as long as the schedule requires.

The risk register is measured against the most recent exercise record. The hardened build is compared with the agreed service level. The remote access path is measured against the agreed service level. The classification scheme is validated by the commissioning document. Testing covers the failure case, not only the happy path.

The patch calendar is reviewed against the commissioning document. The classification scheme is reconciled with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is measured against the register of exceptions. The continuity plan is documented alongside the signed exception log. The procedure is written so a new starter can follow it without supervision.

The recovery test is validated by the previous year's assessment. The endpoint baseline is measured against the previous year's assessment. The backup rotation is reconciled with the agreed service level. The email authentication record is measured against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The vendor register is checked against the dependency map. The recovery test is reconciled with the previous year's assessment. The email authentication record is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

6. The remote access path

The threat model is evidenced by the previous year's assessment. The metric set is compared with the previous year's assessment. The continuity plan is evidenced by the evidence pack held by the owner. The remote access path is checked against the ticket history for the period. Testing covers the failure case, not only the happy path.

The mobile standard is checked against the ticket history for the period. The metric set is documented alongside the signed exception log. The retention schedule is reconciled with the most recent exercise record. The asset register is evidenced by the ticket history for the period. Testing covers the failure case, not only the happy path.

Each administrative account is documented alongside the dependency map. The vendor register is reconciled with the quarterly review notes. The mobile standard is validated by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The recovery test is reviewed against the agreed service level. The classification scheme is reconciled with the previous year's assessment. The third-party register is measured against the commissioning document. The change process is reconciled with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The metric set is validated by the register of exceptions. The threat model is measured against the register of exceptions. The recovery test is documented alongside the register of exceptions. Any deviation requires written approval and an expiry date.

The threat model is measured against the current written standard. The remote access path is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The patch calendar is reconciled with the quarterly review notes. The physical controls is compared with the dependency map. The monitoring pipeline is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reconciled with the approved design baseline. The email authentication record is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

7. The segmentation boundary

The asset register is validated by the dependency map. The vendor register is measured against the current written standard. The identity lifecycle is documented alongside the commissioning document. The control is tested at least once every twelve months.

The identity lifecycle is measured against the agreed service level. The physical controls is reconciled with the quarterly review notes. The classification scheme is documented alongside the agreed service level. The vendor register is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The remote access path is documented alongside the current written standard. The access review process is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is documented alongside the most recent exercise record. The metric set is reviewed against the signed exception log. The access review process is reviewed against the dependency map. The intent is to make the safe path the default rather than an exception.

Each administrative account is compared with the register of exceptions. The identity lifecycle is evidenced by the commissioning document. The risk register is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The third-party register is validated by the most recent exercise record. The third-party register is measured against the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is measured against the signed exception log. The change process is measured against the agreed service level. The encryption standard is reconciled with the approved design baseline. The threat model is evidenced by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is traced to the previous year's assessment. The vendor register is evidenced by the agreed service level. The mobile standard is checked against the previous year's assessment. The encryption standard is reconciled with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The backup rotation is measured against the agreed service level. The monitoring pipeline is documented alongside the signed exception log. Every internet-facing service is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is traced to the commissioning document. The identity lifecycle is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The third-party register is traced to the evidence pack held by the owner. The risk register is documented alongside the dependency map. The vulnerability queue is compared with the dependency map. Testing covers the failure case, not only the happy path.

The recovery test is reviewed against the commissioning document. The backup rotation is traced to the commissioning document. The recovery test is evidenced by the agreed service level. The recovery test is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The segmentation boundary is measured against the register of exceptions. The physical controls is traced to the agreed service level. Every internet-facing service is documented alongside the approved design baseline. The vendor register is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is traced to the commissioning document. The continuity plan is evidenced by the quarterly review notes. The risk register is measured against the agreed service level. Any deviation requires written approval and an expiry date.

The awareness cycle is traced to the approved design baseline. The recovery test is reconciled with the dependency map. The patch calendar is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The encryption standard is compared with the signed exception log. The access review process is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The patch calendar is traced to the most recent exercise record. The recovery test is compared with the most recent exercise record. The retention schedule is compared with the quarterly review notes. The vulnerability queue is validated by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The segmentation boundary is validated by the approved design baseline. The metric set is documented alongside the evidence pack held by the owner. The third-party register is traced to the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The continuity plan is traced to the agreed service level. The access review process is evidenced by the agreed service level. The change process is measured against the commissioning document. The threat model is checked against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is evidenced by the quarterly review notes. The risk register is compared with the quarterly review notes. The backup rotation is documented alongside the dependency map. Evidence is kept for audit, insurance and regulator requests.

The hardened build is measured against the ticket history for the period. The email authentication record is checked against the register of exceptions. The monitoring pipeline is checked against the current written standard. The patch calendar is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The endpoint baseline is measured against the approved design baseline. The access review process is measured against the agreed service level. The retention schedule is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is reconciled with the previous year's assessment. The metric set is compared with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is reconciled with the most recent exercise record. The patch calendar is reconciled with the ticket history for the period. The hardened build is evidenced by the previous year's assessment. The change process is checked against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is measured against the evidence pack held by the owner. The monitoring pipeline is measured against the approved design baseline. The email authentication record is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is checked against the commissioning document. The vulnerability queue is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

8. The metric set

The classification scheme is reviewed against the ticket history for the period. The segmentation boundary is reviewed against the most recent exercise record. The segmentation boundary is measured against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The retention schedule is measured against the previous year's assessment. The third-party register is compared with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reconciled with the quarterly review notes. The awareness cycle is compared with the signed exception log. The remote access path is reconciled with the previous year's assessment. Metrics are reported as trends rather than single data points.

The risk register is measured against the most recent exercise record. The privileged access list is reconciled with the current written standard. The vulnerability queue is reviewed against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the evidence pack held by the owner. The physical controls is measured against the signed exception log. The third-party register is checked against the evidence pack held by the owner. The continuity plan is compared with the current written standard. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is checked against the quarterly review notes. The vendor register is compared with the dependency map. Every internet-facing service is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is reviewed against the most recent exercise record. The privileged access list is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is traced to the ticket history for the period. The metric set is validated by the most recent exercise record. The classification scheme is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The hardened build is evidenced by the most recent exercise record. The physical controls is checked against the previous year's assessment. The risk register is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

Each administrative account is reconciled with the signed exception log. Every internet-facing service is evidenced by the commissioning document. The monitoring pipeline is compared with the current written standard. The access review process is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is reviewed against the current written standard. The privileged access list is measured against the approved design baseline. The access review process is reviewed against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is compared with the approved design baseline. The change process is checked against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The access review process is checked against the dependency map. The continuity plan is traced to the approved design baseline. The privileged access list is reviewed against the signed exception log. The control is tested at least once every twelve months.

The hardened build is measured against the current written standard. The access review process is compared with the evidence pack held by the owner. The vulnerability queue is validated by the dependency map. The segmentation boundary is measured against the most recent exercise record. Records are retained only as long as the schedule requires.