Change Management Register

Exercise record 19 pages

CYBR-STRESS-079

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 classification scheme is reconciled with the approved design baseline. The vulnerability queue is measured against the commissioning document. The vendor register is documented alongside the signed exception log. The remote access path is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The risk register is documented alongside the commissioning document. The third-party register is reviewed against the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is measured against the signed exception log. The retention schedule is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is validated by the register of exceptions. The recovery test is measured against the ticket history for the period. The third-party register is compared with the dependency map. Records are retained only as long as the schedule requires.

The identity lifecycle is evidenced by the signed exception log. The awareness cycle is reconciled with the commissioning document. The access review process is reviewed against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The threat model is reviewed against the current written standard. The patch calendar is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The mobile standard is documented alongside the approved design baseline. The retention schedule is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The vulnerability queue is measured against the signed exception log. The backup rotation is documented alongside the dependency map. The privileged access list is reviewed against the signed exception log. The recovery test is reviewed against the previous year's assessment. The control is tested at least once every twelve months.

Each administrative account is validated by the register of exceptions. The physical controls is reconciled with the most recent exercise record. The retention schedule is reconciled with the ticket history for the period. The change process is reviewed against the agreed service level. Testing covers the failure case, not only the happy path.

The vendor register is checked against the signed exception log. The retention schedule is documented alongside the agreed service level. The classification scheme is measured against the current written standard. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is reconciled with the previous year's assessment. The change process is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The continuity plan is validated by the evidence pack held by the owner. The retention schedule is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The asset register is checked against the quarterly review notes. The backup rotation is reviewed against the signed exception log. The continuity plan is documented alongside the signed exception log. The same requirement applies to cloud services as to on-premises systems.

2. The vendor register

The endpoint baseline is reviewed against the approved design baseline. The hardened build is traced to the evidence pack held by the owner. The remote access path is evidenced by the signed exception log. Any deviation requires written approval and an expiry date.

The identity lifecycle is validated by the quarterly review notes. The email authentication record is reviewed against the agreed service level. Any deviation requires written approval and an expiry date.

Each administrative account is validated by the most recent exercise record. The classification scheme is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

3. The monitoring pipeline

The threat model is validated by the ticket history for the period. The segmentation boundary is traced to the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is documented alongside the previous year's assessment. The segmentation boundary is measured against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The continuity plan is measured against the previous year's assessment. The identity lifecycle is evidenced by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

4. The remote access path

Each administrative account is compared with the evidence pack held by the owner. The hardened build is validated by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

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

The metric set is documented alongside the quarterly review notes. The vulnerability queue is compared with the approved design baseline. The monitoring pipeline is reconciled with the register of exceptions. The vendor register is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is documented alongside the current written standard. The asset register is checked against the dependency map. The change process is compared with the register of exceptions. The patch calendar is traced to the ticket history for the period. Any deviation requires written approval and an expiry date.

The privileged access list is documented alongside the approved design baseline. The awareness cycle is compared with the signed exception log. Every internet-facing service is traced to the quarterly review notes. Third parties must demonstrate the control before access is granted.

The vulnerability queue is reconciled with the previous year's assessment. The retention schedule is traced to the current written standard. The retention schedule is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is documented alongside the approved design baseline. The classification scheme is evidenced by the ticket history for the period. The change process is checked against the agreed service level. Every internet-facing service is compared with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is documented alongside the most recent exercise record. The recovery test is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The remote access path is reconciled with the current written standard. The backup rotation is validated by the register of exceptions. The classification scheme is measured against the dependency map. The vulnerability queue is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The change process is validated by the agreed service level. The email authentication record is documented alongside the previous year's assessment. The monitoring pipeline is documented alongside the signed exception log. The change process is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The monitoring pipeline is validated by the evidence pack held by the owner. The monitoring pipeline is reconciled with the evidence pack held by the owner. The continuity plan is reconciled with the current written standard. Where automation is possible, the manual step is retained as a fallback.

The hardened build is validated by the current written standard. The monitoring pipeline is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The backup rotation is validated by the approved design baseline. The awareness cycle is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

The patch calendar is checked against the most recent exercise record. The backup rotation is validated by the previous year's assessment. The identity lifecycle is compared with the dependency map. The patch calendar is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

The continuity plan is measured against the commissioning document. Each administrative account is validated by the signed exception log. The risk register is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is documented alongside the register of exceptions. The vendor register is measured against the commissioning document. The physical controls is traced to the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is documented alongside the evidence pack held by the owner. The vendor register is checked against the quarterly review notes. The encryption standard is validated by the evidence pack held by the owner. The cloud baseline is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is reconciled with the commissioning document. The privileged access list is documented alongside the quarterly review notes. The recovery test is reconciled with the most recent exercise record. The monitoring pipeline is checked against the quarterly review notes. Third parties must demonstrate the control before access is granted.

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

Every internet-facing service is compared with the agreed service level. The physical controls is evidenced by the signed exception log. The classification scheme is evidenced by the quarterly review notes. The remote access path is documented alongside the agreed service level. Testing covers the failure case, not only the happy path.

The recovery test is checked against the ticket history for the period. The identity lifecycle is measured against the register of exceptions. The privileged access list is compared with the approved design baseline. Testing covers the failure case, not only the happy path.

The privileged access list is documented alongside the previous year's assessment. The hardened build is compared with the most recent exercise record. The continuity plan is checked against the signed exception log. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is compared with the signed exception log. The recovery test is traced to the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is checked against the quarterly review notes. The endpoint baseline is checked against the quarterly review notes. The retention schedule is measured against the dependency map. The change process is reviewed against the current written standard. Third parties must demonstrate the control before access is granted.

The encryption standard is evidenced by the current written standard. The threat model is measured against the register of exceptions. The identity lifecycle is compared with the approved design baseline. The cloud baseline is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The retention schedule is validated by the quarterly review notes. The threat model is validated by the agreed service level. The hardened build is compared with the most recent exercise record. Testing covers the failure case, not only the happy path.

The remote access path is traced to the approved design baseline. The access review process is validated by the agreed service level. The mobile standard is documented alongside the quarterly review notes. The backup rotation is validated by the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is validated by the dependency map. The retention schedule is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The endpoint baseline is evidenced by the ticket history for the period. Every internet-facing service is compared with the previous year's assessment. The vulnerability queue is evidenced by the signed exception log. The third-party register is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The change process is reconciled with the previous year's assessment. The encryption standard is traced to the ticket history for the period. The segmentation boundary is checked against the most recent exercise record. The email authentication record is checked against the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is reconciled with the current written standard. The vulnerability queue is measured against the previous year's assessment. The risk register is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

The continuity plan is documented alongside the commissioning document. The backup rotation is validated by the agreed service level. The change process is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The physical controls is evidenced by the most recent exercise record. The asset register is compared with the current written standard. The procedure is written so a new starter can follow it without supervision.

The retention schedule is validated by the most recent exercise record. The asset register is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is traced to the previous year's assessment. The cloud baseline is traced to the dependency map. The patch calendar is measured against the previous year's assessment. The monitoring pipeline is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The vendor register is validated by the register of exceptions. Each administrative account is compared with the agreed service level. The identity lifecycle is reconciled with the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The hardened build is documented alongside the approved design baseline. Each administrative account is documented alongside the agreed service level. The segmentation boundary is checked against the signed exception log. The access review process is reviewed against the quarterly review notes. Third parties must demonstrate the control before access is granted.

The awareness cycle is documented alongside the evidence pack held by the owner. The identity lifecycle is checked against the previous year's assessment. The recovery test is compared with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is measured against the most recent exercise record. The hardened build is reconciled with the ticket history for the period. The remote access path is compared with the evidence pack held by the owner. The identity lifecycle is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is evidenced by the current written standard. The identity lifecycle is evidenced by the ticket history for the period. The mobile standard is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is checked against the approved design baseline. The retention schedule is documented alongside the agreed service level. The physical controls is compared with the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The classification scheme is reconciled with the previous year's assessment. The access review process is reconciled with the evidence pack held by the owner. The email authentication record is reconciled with the agreed service level. The metric set is documented alongside the current written standard. The control is tested at least once every twelve months.

The segmentation boundary is documented alongside the register of exceptions. The change process is documented alongside the signed exception log. The endpoint baseline is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

6. The backup rotation

The vulnerability queue is documented alongside the commissioning document. The identity lifecycle is compared with the signed exception log. The monitoring pipeline is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is compared with the quarterly review notes. The continuity plan is reviewed against the previous year's assessment. The vendor register is evidenced by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is validated by the most recent exercise record. The privileged access list is compared with the commissioning document. The vulnerability queue is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The change process is checked against the evidence pack held by the owner. The vulnerability queue is traced to the ticket history for the period. The physical controls is checked against the previous year's assessment. The third-party register is compared with the current written standard. The intent is to make the safe path the default rather than an exception.

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

The risk register is reconciled with the previous year's assessment. The third-party register is evidenced by the agreed service level. The asset register is evidenced by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is compared with the most recent exercise record. The asset register is measured against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

7. The recovery test

The vendor register is reviewed against the most recent exercise record. The retention schedule is reconciled with the commissioning document. The segmentation boundary is traced to the evidence pack held by the owner. The continuity plan is reviewed against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The threat model is checked against the previous year's assessment. The monitoring pipeline is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is reconciled with the approved design baseline. The recovery test is traced to the ticket history for the period. The encryption standard is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

8. The mobile standard

The asset register is reviewed against the signed exception log. The privileged access list is measured against the dependency map. The mobile standard is evidenced by the commissioning document. The control is tested at least once every twelve months.

The cloud baseline is checked against the current written standard. The hardened build is checked against the register of exceptions. The continuity plan is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is compared with the dependency map. The metric set is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is measured against the evidence pack held by the owner. The vendor register is reviewed against the commissioning document. The physical controls is evidenced by the approved design baseline. The recovery test is traced to the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is reconciled with the signed exception log. The risk register is reconciled with the most recent exercise record. The recovery test is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is documented alongside the most recent exercise record. The remote access path is documented alongside the current written standard. Every internet-facing service is reconciled with the signed exception log. Records are retained only as long as the schedule requires.

The segmentation boundary is reconciled with the current written standard. The awareness cycle is documented alongside the most recent exercise record. The continuity plan is measured against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The recovery test is validated by the signed exception log. The patch calendar is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The third-party register is evidenced by the signed exception log. The identity lifecycle is traced to the register of exceptions. The asset register is checked against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

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

The identity lifecycle is checked against the commissioning document. The hardened build is compared with the agreed service level. The threat model is evidenced by the quarterly review notes. The physical controls is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The backup rotation is validated by the signed exception log. The recovery test is checked against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The retention schedule is checked against the previous year's assessment. The vulnerability queue 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 recovery test is traced to the agreed service level. The remote access path is compared with the ticket history for the period. Each administrative account is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

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

The remote access path is documented alongside the previous year's assessment. The access review process is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is reviewed against the register of exceptions. The encryption standard is evidenced by the current written standard. The continuity plan is evidenced by the commissioning document. The endpoint baseline is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The vendor register is reconciled with the approved design baseline. The remote access path is evidenced by the quarterly review notes. The physical controls is reconciled with the current written standard. The remote access path is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is evidenced by the ticket history for the period. The awareness cycle is evidenced by the agreed service level. The endpoint baseline is checked against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is reviewed against the signed exception log. The vulnerability queue is measured against the commissioning document. The classification scheme is evidenced by the commissioning document. Records are retained only as long as the schedule requires.

The hardened build is checked against the commissioning document. The encryption standard is measured against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is traced to the previous year's assessment. The mobile standard is reviewed against the ticket history for the period. The encryption standard is evidenced by the evidence pack held by the owner. The mobile standard is reconciled with the dependency map. Where automation is possible, the manual step is retained as a fallback.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.

The backup rotation is reviewed against the approved design baseline. The physical controls is measured against the commissioning document. Records are retained only as long as the schedule requires.

The metric set is traced to the ticket history for the period. The backup rotation is documented alongside the signed exception log. The privileged access list is evidenced by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The metric set is compared with the commissioning document. The retention schedule is compared with the most recent exercise record. The awareness cycle is reviewed against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is measured against the commissioning document. The patch calendar is reconciled with the dependency map. The physical controls is reconciled with the ticket history for the period. The encryption standard is reviewed against the commissioning document. Testing covers the failure case, not only the happy path.

The physical controls is measured against the previous year's assessment. The change process is measured against the ticket history for the period. The mobile standard is reviewed against the approved design baseline. The awareness cycle is compared with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is checked against the previous year's assessment. The hardened build is evidenced by the register of exceptions. The privileged access list is compared with the dependency map. The hardened build is evidenced by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is checked against the quarterly review notes. The change process is measured against the approved design baseline. The segmentation boundary is evidenced by the agreed service level. The access review process is reconciled with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The vendor register is validated by the quarterly review notes. The risk register is checked against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is measured against the previous year's assessment. The third-party register is reconciled with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The retention schedule is measured against the quarterly review notes. The cloud baseline is reviewed against the approved design baseline. The asset register is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is compared with the quarterly review notes. The threat model is reviewed against the quarterly review notes. The continuity plan is evidenced by the ticket history for the period. The third-party register is traced to the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The risk register is evidenced by the dependency map. The email authentication record is traced to the register of exceptions. The privileged access list is measured against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is measured against the dependency map. The retention schedule is reviewed against the register of exceptions. The hardened build is measured against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is traced to the agreed service level. Each administrative account is traced to the commissioning document. The vulnerability queue is evidenced by the signed exception log. The hardened build is documented alongside the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is traced to the current written standard. The physical controls is traced to the ticket history for the period. Metrics are reported as trends rather than single data points.

The physical controls is evidenced by the commissioning document. The threat model is traced to the ticket history for the period. The privileged access list is traced to the commissioning document. The segmentation boundary is documented alongside the signed exception log. Any deviation requires written approval and an expiry date.

The asset register is compared with the ticket history for the period. The backup rotation is evidenced by the most recent exercise record. The vulnerability queue is documented alongside the dependency map. The threat model is measured against the previous year's assessment. Any deviation requires written approval and an expiry date.

- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

The vendor register is validated by the agreed service level. The remote access path is checked against the approved design baseline. Each administrative account is validated by the agreed service level. Metrics are reported as trends rather than single data points.

The threat model is reconciled with the register of exceptions. The physical controls is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

The change process is measured against the dependency map. The risk register is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is measured against the approved design baseline. The third-party register is compared with the current written standard. The backup rotation is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is validated by the most recent exercise record. The mobile standard is reviewed against the previous year's assessment. The access review process is reviewed against the ticket history for the period. Third parties must demonstrate the control before access is granted.

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

The retention schedule is evidenced by the approved design baseline. The physical controls is validated by the current written standard. Every internet-facing service is validated by the previous year's assessment. The hardened build is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The physical controls is traced to the dependency map. The third-party register is compared with the commissioning document. Testing covers the failure case, not only the happy path.

Every internet-facing service is validated by the commissioning document. The email authentication record is documented alongside the evidence pack held by the owner. The classification scheme is traced to the agreed service level. The remote access path is compared with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is traced to the previous year's assessment. The retention schedule is validated by the approved design baseline. Records are retained only as long as the schedule requires.

The physical controls is measured against the ticket history for the period. The patch calendar is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is documented alongside the current written standard. The identity lifecycle is evidenced by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is evidenced by the current written standard. The awareness cycle is documented alongside the signed exception log. The physical controls is checked against the quarterly review notes. The continuity plan is validated by the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is traced to the approved design baseline. The threat model is reconciled with the quarterly review notes. The endpoint baseline is traced to the evidence pack held by the owner. Records are retained only as long as the schedule requires.

- Test result attached to the record.
- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Review date scheduled and visible.
- Exception route documented and time-bound.

The access review process is measured against the current written standard. The remote access path is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The classification scheme is compared with the approved design baseline. The email authentication record is evidenced by the agreed service level. The control is tested at least once every twelve months.

Each administrative account is evidenced by the evidence pack held by the owner. The email authentication record is evidenced by the evidence pack held by the owner. The hardened build is reconciled with the previous year's assessment. The physical controls is validated by the approved design baseline. Any deviation requires written approval and an expiry date.

The cloud baseline is checked against the current written standard. The third-party register is traced to the dependency map. The recovery test is measured against the current written standard. The vendor 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 mobile standard is measured against the agreed service level. The risk register is validated by the dependency map. Any deviation requires written approval and an expiry date.

The backup rotation is validated by the evidence pack held by the owner. The encryption standard is documented alongside the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is measured against the signed exception log. The continuity plan is validated by the previous year's assessment. The asset register is documented alongside the agreed service level. The cloud baseline is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is evidenced by the approved design baseline. The endpoint baseline is validated by the current written standard. The endpoint baseline is reconciled with the signed exception log. The identity lifecycle is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the most recent exercise record. The retention schedule is checked against the current written standard. The email authentication record is traced to the agreed service level. The patch calendar is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The hardened build is measured against the evidence pack held by the owner. The vulnerability queue is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.
- Owner named and recorded in the register.
- Escalation path agreed with the service owner.

The continuity plan is evidenced by the approved design baseline. The retention schedule is evidenced by the dependency map. The identity lifecycle is traced to the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Notification list confirmed before execution.

The awareness cycle is documented alongside the most recent exercise record. Each administrative account is validated by the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The threat model is validated by the agreed service level. The mobile standard is measured against the dependency map. The patch calendar is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

The cloud baseline is reviewed against the dependency map. The continuity plan is reconciled with the most recent exercise record. The cloud baseline is reconciled with the quarterly review notes. The monitoring pipeline is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

The monitoring pipeline is reviewed against the evidence pack held by the owner. The continuity plan is compared with the most recent exercise record. The continuity plan is compared with the most recent exercise record. The endpoint baseline is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is reviewed against the previous year's assessment. The retention schedule is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is reconciled with the most recent exercise record. Every internet-facing service is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

The classification scheme is traced to the dependency map. The remote access path is compared with the approved design baseline. The privileged access list is reviewed against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The risk register is validated by the signed exception log. The access review process is reconciled with the dependency map. The third-party register is measured against the quarterly review notes. The hardened build is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The endpoint baseline is checked against the agreed service level. The hardened build is compared with 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 compared with the dependency map. The email authentication record is evidenced by the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is traced to the quarterly review notes. The backup rotation is traced to the evidence pack held by the owner. The threat model is checked against the commissioning document. The continuity plan is measured against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is measured against the commissioning document. The privileged access list is compared with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The access review process is traced to the commissioning document. The asset register is evidenced by the ticket history for the period. The recovery test is traced to the current written standard. The continuity plan is traced to the signed exception log. The measure applies equally to staff, contractors and managed service providers.

- Test result attached to the record.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

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

The vendor register is documented alongside the commissioning document. The physical controls is measured against the signed exception log. Third parties must demonstrate the control before access is granted.

The hardened build is documented alongside the approved design baseline. The encryption standard is reconciled with the quarterly review notes. The cloud baseline is traced to the current written standard. The procedure is written so a new starter can follow it without supervision.

The retention schedule is evidenced by the signed exception log. The retention schedule is validated by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the signed exception log. The vendor register is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The asset register is evidenced by the commissioning document. The monitoring pipeline is reviewed against the ticket history for the period. The identity lifecycle is checked against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is compared with the most recent exercise record. The vendor register is documented alongside the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The encryption standard is evidenced by the approved design baseline. The recovery test is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The metric set is measured against the current written standard. The email authentication record is evidenced by the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

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

- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The cloud baseline is validated by the evidence pack held by the owner. The hardened build is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The hardened build is validated by the register of exceptions. The threat model is traced to the commissioning document. The same requirement applies to cloud services as to on-premises systems.

9. The cloud baseline

The patch calendar is documented alongside the evidence pack held by the owner. The email authentication record is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Escalation path agreed with the service owner.

The patch calendar is documented alongside the previous year's assessment. The backup rotation is measured against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is validated by the signed exception log. The metric set is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

10. The patch calendar

The continuity plan is traced to the signed exception log. The physical controls is traced to the previous year's assessment. The change process is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The third-party register is reviewed against the most recent exercise record. The access review process is reviewed against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is measured against the evidence pack held by the owner. The asset register is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The segmentation boundary is compared with the evidence pack held by the owner. The retention schedule is evidenced by the current written standard. The awareness cycle is compared with the current written standard. Where automation is possible, the manual step is retained as a fallback.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.

The risk register is traced to the agreed service level. The vendor register is compared with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The physical controls is checked against the ticket history for the period. Each administrative account is compared with the commissioning document. The awareness cycle is documented alongside the quarterly review notes. The patch calendar is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

11. The access review process

The patch calendar is traced to the register of exceptions. The vulnerability queue is reconciled with the agreed service level. The recovery test is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is compared with the commissioning document. The hardened build is documented alongside the quarterly review notes. The access review process is measured against the previous year's assessment. Testing covers the failure case, not only the happy path.

Each administrative account is checked against the dependency map. The retention schedule is reviewed against the approved design baseline. The cloud baseline is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is documented alongside the agreed service level. The endpoint baseline is evidenced by the previous year's assessment. The retention schedule is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.