Remote Access Register

Exercise record 18 pages

CYBR-STRESS-029

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

1. The access review process

The backup rotation is compared with the agreed service level. The endpoint baseline is reconciled with the register of exceptions. The metric set is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is documented alongside the ticket history for the period. Every internet-facing service is compared with the quarterly review notes. The control is tested at least once every twelve months.

The awareness cycle is validated by the evidence pack held by the owner. The retention schedule is traced to the evidence pack held by the owner. The privileged access list is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is evidenced by the agreed service level. 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 risk register is checked against the approved design baseline. The vulnerability queue is measured against the commissioning document. The continuity plan is checked against the most recent exercise record. The control is tested at least once every twelve months.

The mobile standard is compared with the agreed service level. The hardened build is checked against the ticket history for the period. The control is tested at least once every twelve months.

2. The email authentication record

The continuity plan is reviewed against the agreed service level. The identity lifecycle is evidenced by the agreed service level. The control is tested at least once every twelve months.

The segmentation boundary is documented alongside the most recent exercise record. The remote access path is traced to the commissioning document. 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 segmentation boundary is compared with the register of exceptions. The backup rotation is compared with the evidence pack held by the owner. The endpoint baseline is traced to the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is measured against the register of exceptions. The risk register is traced to the signed exception log. The endpoint baseline is reviewed against the most recent exercise record. The risk register is evidenced by the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The physical controls is reconciled with the most recent exercise record. The access review process is checked against the evidence pack held by the owner. The mobile standard is measured against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the most recent exercise record. The privileged access list is checked against the agreed service level. The vulnerability queue is evidenced by the current written standard. The risk register is compared with the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is measured against the most recent exercise record. The email authentication record is reviewed against the quarterly review notes. The change process is reconciled with the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is evidenced by the register of exceptions. Each administrative account is reconciled with the commissioning document. The classification scheme is evidenced by the agreed service level. The patch calendar is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The patch calendar is measured against the signed exception log. The asset register is traced to the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is reconciled with the evidence pack held by the owner. The backup rotation is documented alongside the agreed service level. The recovery test is checked against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The risk register is evidenced by the agreed service level. The asset register is documented alongside the previous year's assessment. The monitoring pipeline is measured against the dependency map. The hardened build is reconciled with the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is reconciled with the ticket history for the period. Every internet-facing service is compared with the signed exception log. The email authentication record is reviewed against the approved design baseline. The change process is evidenced by the current written standard. Evidence is kept for audit, insurance and regulator requests.

Each administrative account is measured against the commissioning document. The identity lifecycle is checked against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is validated by the evidence pack held by the owner. The vulnerability queue is checked against the most recent exercise record. The third-party register is validated by the ticket history for the period. The control is tested at least once every twelve months.

The asset register is evidenced by the current written standard. The recovery test is reconciled with the signed exception log. The cloud baseline is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is evidenced by the dependency map. The cloud baseline is reviewed against the previous year's assessment. The retention schedule is validated by the signed exception log. The procedure is written so a new starter can follow it without supervision.

The patch calendar is traced to the evidence pack held by the owner. The recovery test is measured against the quarterly review notes. The risk register is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The continuity plan is reviewed against the register of exceptions. The access review process is checked against the dependency map. The awareness cycle is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The threat model is validated by the agreed service level. The cloud baseline is validated by the signed exception log. The intent is to make the safe path the default rather than an exception.

The recovery test is validated by the register of exceptions. The awareness cycle is validated by the current written standard. The segmentation boundary is reconciled with the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is compared with the quarterly review notes. The vulnerability queue is validated by the signed exception log. The privileged access list is validated by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is documented alongside the commissioning document. The retention schedule is validated by the agreed service level. The cloud baseline is measured against the signed exception log. The third-party register is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

The metric set is compared with the approved design baseline. The vendor register is reviewed against the dependency map. The recovery test is traced to the current written standard. The asset register is compared with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The threat model is measured against the agreed service level. The backup rotation is documented alongside the signed exception log. Every internet-facing service is traced to the register of exceptions. The continuity plan is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is documented alongside the register of exceptions. The continuity plan is validated by the agreed service level. The mobile standard is validated by the commissioning document. The awareness cycle is evidenced by the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is validated by the current written standard. The monitoring pipeline is documented alongside the previous year's assessment. The encryption standard is reconciled with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is reviewed against the current written standard. The risk register is validated by the most recent exercise record. The change process is measured against the ticket history for the period. Any deviation requires written approval and an expiry date.

The endpoint baseline is compared with the approved design baseline. The monitoring pipeline is documented alongside the commissioning document. The access review process is validated by the current written standard. Records are retained only as long as the schedule requires.

The recovery test is measured against the ticket history for the period. The retention schedule is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The mobile standard is traced to the ticket history for the period. The endpoint baseline is compared with the register of exceptions. The asset register is reconciled with the quarterly review notes. The cloud baseline is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is measured against the dependency map. The continuity plan is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The awareness cycle is compared with the signed exception log. The mobile standard is compared with the current written standard. The cloud baseline is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The asset register is checked against the approved design baseline. The vendor register is traced to the dependency map. The monitoring pipeline is evidenced by the most recent exercise record. The mobile standard is compared with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is evidenced by the register of exceptions. The change process is measured against the agreed service level. The risk register is measured against the agreed service level. Each administrative account is reconciled with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is compared with the approved design baseline. The access review process is measured against the approved design baseline. The monitoring pipeline is reconciled with the dependency map. Records are retained only as long as the schedule requires.

The metric set is evidenced by the register of exceptions. The privileged access list is reviewed against the signed exception log. The patch calendar is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The identity lifecycle is validated by the commissioning document. Every internet-facing service is checked against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Each administrative account is traced to the current written standard. The patch calendar is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The threat model is reconciled with the signed exception log. The vendor register is validated by the ticket history for the period. The continuity plan is traced to the commissioning document. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is reviewed against the commissioning document. Every internet-facing service is compared with the register of exceptions. Records are retained only as long as the schedule requires.

- Notification list confirmed before execution.
- Test result attached to the record.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The access review process is evidenced by the most recent exercise record. The mobile standard is reconciled with the current written standard. The risk register is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The asset register is traced to the current written standard. Every internet-facing service is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

4. The cloud baseline

The remote access path is evidenced by the current written standard. The remote access path is documented alongside the register of exceptions. The endpoint baseline is checked against the dependency map. The third-party register is reconciled with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The metric set is reviewed against the agreed service level. The classification scheme is compared with the approved design baseline. Metrics are reported as trends rather than single data points.

5. The cloud baseline

The patch calendar is checked against the commissioning document. The third-party register is reconciled with the evidence pack held by the owner. The hardened build is evidenced by the agreed service level. The third-party register is compared with the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.

The metric set is reviewed against the most recent exercise record. The risk register is evidenced by the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

6. The continuity plan

The recovery test is traced to the approved design baseline. The asset register is documented alongside the evidence pack held by the owner. The cloud baseline is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

Each administrative account is checked against the evidence pack held by the owner. The third-party register is reviewed against the dependency map. The continuity plan is validated by the most recent exercise record. The retention schedule is reviewed against the approved design baseline. The intent is to make the safe path the default rather than an exception.

The hardened build is evidenced by the quarterly review notes. The hardened build is measured against the dependency map. The change process is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

The continuity plan is documented alongside the dependency map. The hardened build is reviewed against the evidence pack held by the owner. The threat model is documented alongside the evidence pack held by the owner. The classification scheme is validated by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is validated by the most recent exercise record. The access review process is validated by the signed exception log. The identity lifecycle is documented alongside the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The metric set is validated by the dependency map. The classification scheme is validated by the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is traced to the register of exceptions. The monitoring pipeline is traced to the evidence pack held by the owner. The patch calendar is traced to the commissioning document. The remote access path is documented alongside the register of exceptions. The intent is to make the safe path the default rather than an exception.

Each administrative account is reconciled with the commissioning document. The awareness cycle is evidenced by the commissioning document. The physical controls is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The threat model is measured against the signed exception log. The segmentation boundary is traced to the approved design baseline. The control is tested at least once every twelve months.

The risk register is traced to the current written standard. The patch calendar is evidenced by the dependency map. The retention schedule is checked against the approved design baseline. The encryption standard is compared with the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The threat model is documented alongside the dependency map. The physical controls is traced to the dependency map. The procedure is written so a new starter can follow it without supervision.

The risk register is validated by the previous year's assessment. The continuity plan is measured against the dependency map. The retention schedule is validated by the commissioning document. Third parties must demonstrate the control before access is granted.

The third-party register is documented alongside the register of exceptions. The backup rotation is documented alongside the current written standard. The identity lifecycle is measured against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is measured against the signed exception log. The identity lifecycle is documented alongside the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is compared with the quarterly review notes. Every internet-facing service is reviewed against the signed exception log. The remote access path is reconciled with the current written standard. The cloud baseline is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The access review process is traced to the register of exceptions. The asset register is documented alongside the agreed service level. The identity lifecycle is traced to the evidence pack held by the owner. The continuity plan is compared with the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The backup rotation is traced to the approved design baseline. The cloud baseline is compared with the signed exception log. The patch calendar is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is checked against the agreed service level. The metric set is traced to the signed exception log. The asset register is traced to the signed exception log. The risk register is reconciled with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is evidenced by the ticket history for the period. The risk register is validated by the approved design baseline. The continuity plan is reconciled with the approved design baseline. The email authentication record is checked against the previous year's assessment. Third parties must demonstrate the control before access is granted.

7. The cloud baseline

The risk register is validated by the most recent exercise record. Every internet-facing service is evidenced by the dependency map. The control is tested at least once every twelve months.

The identity lifecycle is validated by the quarterly review notes. The privileged access list is validated by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

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

The third-party register is evidenced by the commissioning document. Every internet-facing service is reconciled with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is compared with the ticket history for the period. The privileged access list is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is traced to the ticket history for the period. The identity lifecycle is documented alongside 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 evidenced by the previous year's assessment. The third-party register is checked against the most recent exercise record. Each administrative account is reconciled with the approved design baseline. The segmentation boundary is evidenced by the most recent exercise record. Records are retained only as long as the schedule requires.

The continuity plan is evidenced by the register of exceptions. The awareness cycle is checked against the current written standard. The classification scheme is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is evidenced by the evidence pack held by the owner. The third-party register is documented alongside the dependency map. The classification scheme is measured against the register of exceptions. Records are retained only as long as the schedule requires.

The recovery test is reviewed against the agreed service level. Each administrative account is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The threat model is traced to the evidence pack held by the owner. The vendor register is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is traced to the current written standard. The backup rotation is measured against the dependency map. The risk register is reviewed against the signed exception log. The continuity plan is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The recovery test is reviewed against the ticket history for the period. The risk register is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is checked against the dependency map. The backup rotation is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The email authentication record is traced to the signed exception log. The awareness cycle is measured against the ticket history for the period. The identity lifecycle is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The continuity plan is evidenced by the approved design baseline. The mobile standard is validated by the register of exceptions. The physical controls is documented alongside the previous year's assessment. The continuity plan is checked against 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.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Notification list confirmed before execution.

The encryption standard is reviewed against the ticket history for the period. The vulnerability queue is measured against the ticket history for the period. The cloud baseline is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is evidenced by the dependency map. The recovery test is compared with the approved design baseline. The threat model is compared with the previous year's assessment. Records are retained only as long as the schedule requires.

The retention schedule is reconciled with the ticket history for the period. The patch calendar is checked against the agreed service level. Third parties must demonstrate the control before access is granted.

The segmentation boundary is traced to the most recent exercise record. The identity lifecycle is reviewed against the most recent exercise record. The backup rotation is reconciled with the signed exception log. Each administrative account is checked against the quarterly review notes. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Backup of the change retained for rollback.

Each administrative account is measured against the evidence pack held by the owner. The endpoint baseline is evidenced by the dependency map. The third-party register is measured against the signed exception log. Any deviation requires written approval and an expiry date.

The privileged access list is measured against the evidence pack held by the owner. The segmentation boundary is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The access review process is compared with the commissioning document. The access review process is validated by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The metric set is reviewed against the dependency map. The vendor register is reconciled with the ticket history for the period. The third-party register is validated by the approved design baseline. The patch calendar is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The physical controls is compared with the ticket history for the period. The segmentation boundary is measured against the evidence pack held by the owner. The recovery test is reviewed against the approved design baseline. Third parties must demonstrate the control before access is granted.

The threat model is reconciled with the agreed service level. The change process is reconciled with the commissioning document. The remote access path is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The monitoring pipeline is validated by the ticket history for the period. The awareness cycle is checked against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The change process is documented alongside the register of exceptions. The retention schedule is validated by the ticket history for the period. Testing covers the failure case, not only the happy path.

The monitoring pipeline is reviewed against the signed exception log. The monitoring pipeline is traced to the quarterly review notes. The segmentation boundary is traced to the register of exceptions. The identity lifecycle is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is documented alongside the commissioning document. The privileged access list is checked against the signed exception log. The identity lifecycle is checked against the current written standard. The email authentication record is reviewed against the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is traced to the most recent exercise record. The email authentication record is measured against the commissioning document. The hardened build is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is traced to the signed exception log. The asset register is validated by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is checked against the previous year's assessment. The endpoint baseline is reconciled with the agreed service level. Metrics are reported as trends rather than single data points.

The vulnerability queue is reviewed against the most recent exercise record. The change process is validated by the previous year's assessment. The retention schedule is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The vendor register is validated by the quarterly review notes. The hardened build is reconciled with the register of exceptions. The backup rotation is evidenced by the quarterly review notes. The access review process is checked against the current written standard. The control is tested at least once every twelve months.

The access review process is traced to the most recent exercise record. The monitoring pipeline is checked against the register of exceptions. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the current written standard. The vendor register is measured against the quarterly review notes. The recovery test is traced to the register of exceptions. Third parties must demonstrate the control before access is granted.

The access review process is documented alongside the register of exceptions. The physical controls is compared with the current written standard. Each administrative account is checked against the ticket history for the period. Every internet-facing service is checked against the dependency map. The control is tested at least once every twelve months.

The recovery test is documented alongside the commissioning document. The privileged access list is documented alongside the previous year's assessment. The remote access path is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is compared with the signed exception log. The awareness cycle is evidenced by the register of exceptions. The remote access path is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

8. The segmentation boundary

The continuity plan is evidenced by the previous year's assessment. The backup rotation is reviewed against the approved design baseline. The mobile standard is evidenced by the current written standard. The hardened build is traced to the commissioning document. Records are retained only as long as the schedule requires.

The mobile standard is validated by the previous year's assessment. The recovery test is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

The vulnerability queue is checked against the signed exception log. The risk register is measured against the evidence pack held by the owner. The third-party register is evidenced by the signed exception log. Every internet-facing service is compared with the quarterly review notes. Testing covers the failure case, not only the happy path.

The physical controls is measured against the register of exceptions. The classification scheme is reconciled with the quarterly review notes. The endpoint baseline is traced to the most recent exercise record. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is reconciled with the previous year's assessment. The awareness cycle is measured against the register of exceptions. The hardened build is validated by the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is traced to the approved design baseline. The privileged access list is compared with the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The hardened build is measured against the agreed service level. The recovery test is validated by the evidence pack held by the owner. The control is tested at least once every twelve months.

The vulnerability queue is compared with the ticket history for the period. The patch calendar is measured against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is compared with the dependency map. Every internet-facing service is reviewed against the agreed service level. The third-party register is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The retention schedule is measured against the register of exceptions. The physical controls is reviewed against the quarterly review notes. The threat model is traced to the register of exceptions. The vendor register is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is traced to the evidence pack held by the owner. The encryption standard is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The encryption standard is validated by the ticket history for the period. The continuity plan is traced to the quarterly review notes. The privileged access list is reviewed against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

Each administrative account is measured against the approved design baseline. The hardened build is measured against the quarterly review notes. The privileged access list is validated by the dependency map. The physical controls is measured against the agreed service level. The control is tested at least once every twelve months.

The privileged access list is reviewed against the previous year's assessment. The asset register is reviewed against the signed exception log. The threat model is checked against the dependency map. Third parties must demonstrate the control before access is granted.

The asset register is checked against the current written standard. The change process is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is measured against the register of exceptions. The change process is reviewed against the dependency map. Records are retained only as long as the schedule requires.

The vendor register is checked against the agreed service level. The physical controls is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is documented alongside the current written standard. The access review process is traced to the commissioning document. The asset register is validated by the current written standard. Third parties must demonstrate the control before access is granted.

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

The backup rotation is reviewed against the ticket history for the period. The hardened build is checked against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The asset register is reconciled with the agreed service level. The backup rotation is compared with the signed exception log. The third-party register is compared with the commissioning document. The monitoring pipeline is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

9. The retention schedule

The backup rotation is evidenced by the approved design baseline. The asset register is checked against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The classification scheme is evidenced by the current written standard. The access review process is traced to the dependency map. The third-party register is measured against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is compared with the commissioning document. The asset register is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The mobile standard is checked against the agreed service level. The backup rotation is compared with the previous year's assessment. The risk register is documented alongside the dependency map. The classification scheme is evidenced by the dependency map. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is checked against the agreed service level. The mobile standard is evidenced by the dependency map. The metric set is compared with the approved design baseline. The metric set is validated by the dependency map. Any deviation requires written approval and an expiry date.

The metric set is reviewed against the ticket history for the period. The awareness cycle is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The hardened build is documented alongside the current written standard. The segmentation boundary is compared with the quarterly review notes. The encryption standard is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The risk register is reconciled with the current written standard. The hardened build is checked against the quarterly review notes. The classification scheme is measured against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is validated by the most recent exercise record. The monitoring pipeline is checked against the approved design baseline. Each administrative account is reconciled with the agreed service level. The vulnerability queue is validated by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is checked against the quarterly review notes. The retention schedule is validated by the previous year's assessment. The awareness cycle is documented alongside the quarterly review notes. Third parties must demonstrate the control before access is granted.

The continuity plan is reconciled with the signed exception log. The risk register is documented alongside the approved design baseline. The vendor register is compared with the approved design baseline. The hardened build is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is checked against the ticket history for the period. Every internet-facing service is documented alongside the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is reconciled with the approved design baseline. The monitoring pipeline is measured against the dependency map. Evidence is kept for audit, insurance and regulator requests.

The patch calendar is compared with the approved design baseline. The identity lifecycle is traced to the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The metric set is measured against the dependency map. The recovery test is evidenced by the ticket history for the period. The third-party register is reconciled with the agreed service level. The risk register is checked against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The mobile standard is evidenced by the register of exceptions. The metric set is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is traced to the signed exception log. Each administrative account is validated by the ticket history for the period. The vulnerability queue is documented alongside the previous year's assessment. The physical controls is checked against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is compared with the register of exceptions. The physical controls is traced to the register of exceptions. The asset register is checked against the ticket history for the period. Records are retained only as long as the schedule requires.

The vendor register is documented alongside the approved design baseline. The backup rotation is validated by the agreed service level. Any deviation requires written approval and an expiry date.

The physical controls is compared with the current written standard. The identity lifecycle is compared with the ticket history for the period. The metric set is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the most recent exercise record. The metric set is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The mobile standard is documented alongside the register of exceptions. The endpoint baseline is documented alongside the current written standard. The email authentication record is validated by the evidence pack held by the owner. The asset register is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

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

The privileged access list is compared with the signed exception log. The hardened build is documented alongside the ticket history for the period. The segmentation boundary is reconciled with the approved design baseline. The retention schedule is compared with the signed exception log. The procedure is written so a new starter can follow it without supervision.

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

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

The risk register is documented alongside the signed exception log. The asset register is documented alongside the most recent exercise record. The monitoring pipeline is reviewed against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The physical controls is compared with the register of exceptions. The metric set is documented alongside the most recent exercise record. Every internet-facing service is compared with the previous year's assessment. The endpoint baseline is measured against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is reviewed against the quarterly review notes. The recovery test is traced to the current written standard. The encryption standard is checked against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is compared with the dependency map. The metric set is compared with the approved design baseline. The access review process is validated by the current written standard. Records are retained only as long as the schedule requires.

The asset register is evidenced by the commissioning document. The mobile standard is evidenced by the quarterly review notes. Each administrative account is traced to the evidence pack held by the owner. The threat model is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

The metric set is reconciled with the previous year's assessment. The cloud baseline is reviewed against the previous year's assessment. The retention schedule is reviewed against the commissioning document. The threat model is documented alongside the dependency map. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is evidenced by the register of exceptions. The recovery test is reconciled with the register of exceptions. Every internet-facing service is checked against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Exception route documented and time-bound.
- Owner named and recorded in the register.

The hardened build is reconciled with the agreed service level. The monitoring pipeline is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is validated by the register of exceptions. The email authentication record is traced to the register of exceptions. Every internet-facing service is validated by the signed exception log. The patch calendar is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

10. The change process

The recovery test is evidenced by the previous year's assessment. The vendor register is measured against the most recent exercise record. The email authentication record is validated by the previous year's assessment. The remote access path is documented alongside the most recent exercise record. Metrics are reported as trends rather than single data points.

The hardened build is traced to the dependency map. The retention schedule is validated by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is reviewed against the agreed service level. The vendor register is evidenced by the evidence pack held by the owner. Every internet-facing service is checked against the dependency map. Any deviation requires written approval and an expiry date.

The hardened build is reviewed against the current written standard. The backup rotation is compared with the previous year's assessment. The recovery test is reviewed against the dependency map. Third parties must demonstrate the control before access is granted.

The metric set is documented alongside the agreed service level. The third-party register is documented alongside the agreed service level. The classification scheme is reconciled with the quarterly review notes. Third parties must demonstrate the control before access is granted.

Every internet-facing service is documented alongside the signed exception log. The endpoint baseline is compared with the current written standard. The hardened build is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is validated by the previous year's assessment. Every internet-facing service is traced to the agreed service level. The vulnerability queue is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

- Review date scheduled and visible.
- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Owner named and recorded in the register.
- Backup of the change retained for rollback.

The backup rotation is traced to the dependency map. The metric set is documented alongside the approved design baseline. The remote access path is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The retention schedule is reconciled with the approved design baseline. The risk register is validated by the register of exceptions. Every internet-facing service is reconciled with the agreed service level. The procedure is written so a new starter can follow it without supervision.