Disaster Recovery Programme

Procedure 16 pages

CYBR-STRESS-006

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 metric set is evidenced by the ticket history for the period. The email authentication record is compared with the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is validated by the register of exceptions. The classification scheme is validated by the quarterly review notes. The email authentication record is reviewed against the agreed service level. The continuity plan is compared with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The email authentication record is validated by the evidence pack held by the owner. The third-party register is evidenced by the ticket history for the period. The asset register is validated by the most recent exercise record. The cloud baseline is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is validated by the quarterly review notes. The continuity plan is reviewed against the register of exceptions. The endpoint baseline is reviewed against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The metric set is reviewed against the commissioning document. The recovery test is reconciled with the quarterly review notes. The remote access path is documented alongside the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The risk register is measured against the dependency map. The cloud baseline is reviewed against the quarterly review notes. The email authentication record is validated by the agreed service level. The identity lifecycle is measured against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

The cloud baseline is traced to the approved design baseline. The classification scheme is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is checked against the signed exception log. The mobile standard is measured against the dependency map. The vulnerability queue is compared with the current written standard. The control is tested at least once every twelve months.

The segmentation boundary is evidenced by the approved design baseline. The mobile standard is compared with the evidence pack held by the owner. Each administrative account is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The patch calendar is validated by the quarterly review notes. The segmentation boundary is reconciled with the previous year's assessment. Any deviation requires written approval and an expiry date.

1. The awareness cycle

The risk register is measured against the dependency map. The risk register is validated by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is validated by the commissioning document. The threat model is measured against the previous year's assessment. Any deviation requires written approval and an expiry date.

The asset register is traced to the register of exceptions. The cloud baseline is compared with the quarterly review notes. The continuity plan is reviewed against the current written standard. The endpoint baseline is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The mobile standard is measured against the evidence pack held by the owner. The retention schedule is compared with the signed exception log. The intent is to make the safe path the default rather than an exception.

The hardened build is evidenced by the quarterly review notes. Each administrative account is documented alongside the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is reconciled with the most recent exercise record. The risk register is compared with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The recovery test is validated by the commissioning document. The backup rotation is documented alongside the dependency map. The hardened build is reviewed against the previous year's assessment. The monitoring pipeline is documented alongside the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

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

Every internet-facing service is evidenced by the current written standard. The email authentication record is compared with the commissioning document. The classification scheme is reconciled with the commissioning document. The vulnerability queue is checked against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

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

The threat model is reviewed against the evidence pack held by the owner. The identity lifecycle is documented alongside the approved design baseline. Every internet-facing service is evidenced by the dependency map. Each administrative account is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The access review process is reconciled with the most recent exercise record. The classification scheme is compared with the dependency map. The segmentation boundary is validated by the ticket history for the period. The continuity plan is reconciled with the approved design baseline. The control is tested at least once every twelve months.

The email authentication record is compared with the signed exception log. The hardened build is checked against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The threat model is measured against the approved design baseline. The monitoring pipeline is traced to the signed exception log. The classification scheme is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is validated by the dependency map. The threat model is documented alongside the register of exceptions. The risk register is reviewed against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is evidenced by the quarterly review notes. The retention schedule is checked against the most recent exercise record. The threat model is evidenced by the dependency map. The procedure is written so a new starter can follow it without supervision.

The physical controls is evidenced by the agreed service level. The mobile standard is reconciled with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is compared with the register of exceptions. The privileged access list is evidenced by the most recent exercise record. The metric set is reconciled with the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is compared with the previous year's assessment. The backup rotation is reconciled with the quarterly review notes. The physical controls is validated by the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is validated by the commissioning document. The cloud baseline is reviewed against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.

The patch calendar is evidenced by the evidence pack held by the owner. The asset register is reviewed against the register of exceptions. The privileged access list is documented alongside the ticket history for the period. The hardened build is documented alongside the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The access review process is validated by the signed exception log. The change process is compared with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is reconciled with the current written standard. The vendor register is measured against the register of exceptions. The email authentication record is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The threat model is compared with the register of exceptions. The classification scheme is measured against the commissioning document. The asset register is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is evidenced by the signed exception log. Every internet-facing service is checked against the commissioning document. The continuity plan is documented alongside the signed exception log. The backup rotation is checked against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The vendor register is reconciled with the current written standard. The remote access path is reviewed against the approved design baseline. Every internet-facing service is checked against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is validated by the agreed service level. The metric set is reviewed against the most recent exercise record. Records are retained only as long as the schedule requires.

The third-party register is evidenced by the dependency map. The hardened build is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is measured against the approved design baseline. The recovery test is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is validated by the signed exception log. The identity lifecycle is evidenced by the agreed service level. The threat model is compared with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The risk register is compared with the quarterly review notes. The mobile standard is compared with the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The recovery test is documented alongside the commissioning document. The patch calendar is traced to the register of exceptions. Each administrative account is evidenced by the ticket history for the period. The metric set is reconciled with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is reconciled with the most recent exercise record. Every internet-facing service is checked against the current written standard. The third-party register is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is reviewed against the quarterly review notes. The encryption standard is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The asset register is reconciled with the current written standard. The endpoint baseline is traced to the previous year's assessment. The identity lifecycle is documented alongside the dependency map. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is validated by the signed exception log. The risk register is reviewed against the quarterly review notes. The recovery test is measured against the approved design baseline. The access review process is reviewed against the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is validated by the quarterly review notes. The access review process is compared with the previous year's assessment. The backup rotation is documented alongside the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The threat model is validated by the ticket history for the period. The continuity plan is validated by the agreed service level. The control is tested at least once every twelve months.

2. The risk register

The third-party register is reconciled with the previous year's assessment. The vulnerability queue 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 remote access path is documented alongside the ticket history for the period. The retention schedule is checked against the agreed service level. The monitoring pipeline is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is reconciled with the dependency map. The endpoint baseline is reconciled with the dependency map. Third parties must demonstrate the control before access is granted.

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

3. The segmentation boundary

The patch calendar is compared with the agreed service level. The recovery test is documented alongside the most recent exercise record. The email authentication record is reconciled with the agreed service level. The metric set is validated by the current written standard. The intent is to make the safe path the default rather than an exception.

The vendor register is checked against the evidence pack held by the owner. The encryption standard is traced to the signed exception log. The endpoint baseline is checked against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is validated by the commissioning document. Every internet-facing service is traced to the most recent exercise record. The hardened build is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is compared with the quarterly review notes. The vulnerability queue is checked against the register of exceptions. The access review process is evidenced by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is reviewed against the previous year's assessment. The access review process is measured against the previous year's assessment. The encryption standard is reviewed against the approved design baseline. The risk register is documented alongside the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is documented alongside the register of exceptions. The vulnerability queue is compared with the quarterly review notes. The metric set is compared with the signed exception log. The encryption standard is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

4. The physical controls

The cloud baseline is compared with the evidence pack held by the owner. The physical controls is validated by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is measured against the agreed service level. The access review process is validated by the evidence pack held by the owner. Records are retained only as long as the schedule requires.

Each administrative account is measured against the signed exception log. The endpoint baseline is compared with the evidence pack held by the owner. Each administrative account is traced to the commissioning document. The endpoint baseline is evidenced by the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

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

The access review process is reconciled with the quarterly review notes. The continuity plan is reconciled with the commissioning document. The vulnerability queue is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The remote access path is validated by the approved design baseline. The mobile standard is documented alongside the agreed service level. Metrics are reported as trends rather than single data points.

The patch calendar is measured against the dependency map. The change process is compared with the agreed service level. Any deviation requires written approval and an expiry date.

The continuity plan is measured against the current written standard. The identity lifecycle is compared with the agreed service level. Each administrative account is traced to the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The email authentication record is evidenced by the quarterly review notes. The monitoring pipeline is validated by the ticket history for the period. The segmentation boundary is traced to the current written standard. The mobile standard 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 email authentication record is measured against the previous year's assessment. Each administrative account is reconciled with the ticket history for the period. The backup rotation is validated by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is reviewed against the ticket history for the period. The hardened build is traced to the dependency map. The access review process is documented alongside the evidence pack held by the owner. The email authentication record is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The cloud baseline is evidenced by the current written standard. The third-party register is checked against the dependency map. The vendor register is evidenced by the ticket history for the period. Any deviation requires written approval and an expiry date.

The vendor register is reviewed against the approved design baseline. The risk register is documented alongside the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The privileged access list is traced to the register of exceptions. The hardened build is reviewed against the current written standard. Third parties must demonstrate the control before access is granted.

The cloud baseline is documented alongside the agreed service level. The mobile standard is reconciled with the signed exception log. The email authentication record is measured against the current written standard. The third-party register is reviewed against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is reviewed against the dependency map. The remote access path is measured against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is traced to the quarterly review notes. The third-party register is reviewed against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

- Owner named and recorded in the register.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

The identity lifecycle is compared with the evidence pack held by the owner. The remote access path is reconciled with the dependency map. The vendor register is documented alongside the quarterly review notes. The mobile standard is checked against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is validated by the evidence pack held by the owner. The change process is validated by the register of exceptions. The backup rotation is compared with the quarterly review notes. Any deviation requires written approval and an expiry date.

The change process is evidenced by the signed exception log. The recovery test is traced to the current written standard. The continuity plan is checked against the dependency map. Metrics are reported as trends rather than single data points.

The vulnerability queue is compared with the register of exceptions. The monitoring pipeline is evidenced by the current written standard. The continuity plan is measured against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reconciled with the commissioning document. Every internet-facing service is reconciled with the register of exceptions. Testing covers the failure case, not only the happy path.

The classification scheme is evidenced by the current written standard. The mobile standard is validated by the agreed service level. The change process is documented alongside the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is reviewed against the approved design baseline. The metric set is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The classification scheme is checked against the previous year's assessment. The vulnerability queue is measured against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The access review process is traced to the commissioning document. The metric set is evidenced by the commissioning document. Records are retained only as long as the schedule requires.

The physical controls is traced to the quarterly review notes. The vulnerability queue is checked against the current written standard. Every internet-facing service is documented alongside the dependency map. Any deviation requires written approval and an expiry date.

The hardened build is documented alongside the commissioning document. The hardened build is traced to the current written standard. The hardened build is measured against the dependency map. Any deviation requires written approval and an expiry date.

The patch calendar is measured against the agreed service level. The monitoring pipeline is checked against the most recent exercise record. The continuity plan is reviewed against the dependency map. The control is tested at least once every twelve months.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.

The vendor register is validated by the most recent exercise record. The asset register is measured against the previous year's assessment. The identity lifecycle is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

The identity lifecycle is evidenced by the agreed service level. The retention schedule is validated by the dependency map. The physical controls is traced to the agreed service level. The privileged access list is compared with the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is reviewed against the agreed service level. The monitoring pipeline is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

Each administrative account is traced to the register of exceptions. The recovery test is documented alongside the agreed service level. The awareness cycle is compared with the dependency map. Third parties must demonstrate the control before access is granted.

Each administrative account is measured against the signed exception log. The classification scheme is compared with the quarterly review notes. The asset register is measured against the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is reviewed against the dependency map. The endpoint baseline is reviewed against the most recent exercise record. The access review process is validated by the most recent exercise record. The risk register is evidenced by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

Every internet-facing service is measured against the agreed service level. The change process is evidenced by the current written standard. Each administrative account is compared with the signed exception log. The backup rotation is documented alongside the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

5. Each administrative account

The vulnerability queue is evidenced by the quarterly review notes. The recovery test is validated by the signed exception log. Every internet-facing service is compared with the quarterly review notes. Records are retained only as long as the schedule requires.

The hardened build is compared with the agreed service level. The metric set is measured against the most recent exercise record. The risk register is measured against the current written standard. The identity lifecycle is checked against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is measured against the quarterly review notes. The patch calendar is traced to the ticket history for the period. The privileged access list is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The threat model is validated by the ticket history for the period. The retention schedule is traced to the quarterly review notes. Each administrative account is reviewed against the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is documented alongside the current written standard. The access review process is validated by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is compared with the signed exception log. The physical controls is evidenced by the agreed service level. The recovery test is traced to the dependency map. The intent is to make the safe path the default rather than an exception.

The recovery test is checked against the dependency map. The backup rotation is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is checked against the ticket history for the period. The awareness cycle is measured against the evidence pack held by the owner. The risk register is reconciled with the current written standard. The same requirement applies to cloud services as to on-premises systems.

The continuity plan is checked against the previous year's assessment. The classification scheme is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reviewed against the dependency map. The risk register is reviewed against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The access review process is checked against the commissioning document. The cloud baseline is traced to the register of exceptions. The privileged access list is checked against the signed exception log. The mobile standard is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The continuity plan is validated by the register of exceptions. The endpoint baseline is documented alongside the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The access review process is documented alongside the signed exception log. The physical controls is checked against the dependency map. The privileged access list is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is reconciled with the approved design baseline. Each administrative account is reconciled with the ticket history for the period. The physical controls is measured against the commissioning document. The awareness cycle is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is traced to the agreed service level. The vulnerability queue is checked against the agreed service level. Every internet-facing service is documented alongside the agreed service level. Metrics are reported as trends rather than single data points.

The asset register is checked against the quarterly review notes. The awareness cycle is measured against the commissioning document. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is validated by the commissioning document. The risk register is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is measured against the quarterly review notes. Each administrative account is compared with the quarterly review notes. The vendor register is traced to the previous year's assessment. Testing covers the failure case, not only the happy path.

The vendor register is compared with the current written standard. The asset register is documented alongside the current written standard. The continuity plan is traced to the register of exceptions. Metrics are reported as trends rather than single data points.

Every internet-facing service is reconciled with the agreed service level. The third-party register is validated by the evidence pack held by the owner. The recovery test is documented alongside the signed exception log. The backup rotation is checked against the dependency map. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is measured against the dependency map. The threat model is reconciled with the previous year's assessment. The cloud baseline is reviewed against the agreed service level. The hardened build is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

The metric set is reviewed against the ticket history for the period. The recovery test is traced to the quarterly review notes. The endpoint baseline is measured against the dependency map. Any deviation requires written approval and an expiry date.

The backup rotation is compared with the agreed service level. The hardened build is measured against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

- Evidence stored in the shared evidence pack.
- Review date scheduled and visible.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The endpoint baseline is evidenced by the quarterly review notes. The threat model is reviewed against the approved design baseline. The endpoint baseline is validated by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is documented alongside the signed exception log. The patch calendar is measured against the signed exception log. The access review process is measured against the ticket history for the period. The backup rotation is reconciled with the dependency map. The control is tested at least once every twelve months.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.
- Review date scheduled and visible.

Every internet-facing service is checked against the dependency map. The physical controls is compared with the register of exceptions. The continuity plan is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The hardened build is documented alongside the dependency map. The third-party register is measured against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The remote access path is compared with the dependency map. The third-party register is documented alongside the current written standard. The risk register is reconciled with the quarterly review notes. The awareness cycle is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The patch calendar is reconciled with the current written standard. The risk register is checked against the register of exceptions. Each administrative account is reviewed against the register of exceptions. The risk register is validated by the previous year's assessment. Testing covers the failure case, not only the happy path.

The recovery test is documented alongside the quarterly review notes. The third-party register is compared with the current written standard. The segmentation boundary is checked against the agreed service level. Each administrative account is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is checked against the approved design baseline. The patch calendar is validated by the dependency map. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is traced to the agreed service level. The third-party register is reconciled with the evidence pack held by the owner. The recovery test is measured against the agreed service level. The vulnerability queue is evidenced by the agreed service level. The control is tested at least once every twelve months.

The retention schedule is compared with the approved design baseline. The recovery test is evidenced by the register of exceptions. The recovery test is checked against the current written standard. The vendor register is evidenced by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The mobile standard is reconciled with the register of exceptions. The monitoring pipeline is evidenced by the commissioning document. The segmentation boundary is validated by the ticket history for the period. Each administrative account is documented alongside the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The patch calendar is traced to the ticket history for the period. The change process is evidenced by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is documented alongside the commissioning document. The segmentation boundary is reviewed against the previous year's assessment. Metrics are reported as trends rather than single data points.

The change process is compared with the most recent exercise record. The change process is evidenced by the approved design baseline. The privileged access list is reconciled with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.
- Test result attached to the record.

The vulnerability queue is evidenced by the evidence pack held by the owner. The email authentication record is documented alongside the quarterly review notes. The patch calendar is checked against the dependency map. Third parties must demonstrate the control before access is granted.

The segmentation boundary is reconciled with the signed exception log. Each administrative account is reviewed against the quarterly review notes. The mobile standard is traced to the current written standard. The change process is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The vulnerability queue is traced to the approved design baseline. The continuity plan is documented alongside the dependency map. The identity lifecycle is compared with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is validated by the agreed service level. The cloud baseline is evidenced by the register of exceptions. The vulnerability queue is documented alongside the signed exception log. Metrics are reported as trends rather than single data points.

The mobile standard is validated by the current written standard. The change process is validated by the signed exception log. The identity lifecycle is checked against the most recent exercise record. The control is tested at least once every twelve months.

The mobile standard is measured against the ticket history for the period. The vendor register is documented alongside the approved design baseline. The endpoint baseline is validated by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The asset register is traced to the signed exception log. The email authentication record is reconciled with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is compared with the current written standard. The privileged access list is documented alongside the most recent exercise record. The change process is checked against the dependency map. Third parties must demonstrate the control before access is granted.

The remote access path is reviewed against the previous year's assessment. The hardened build is documented alongside the agreed service level. The vulnerability queue is compared with the dependency map. The metric set is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The retention schedule is measured against the commissioning document. The vulnerability queue is measured against the most recent exercise record. Testing covers the failure case, not only the happy path.

Every internet-facing service is reconciled with the previous year's assessment. Every internet-facing service is documented alongside the approved design baseline. The change process is checked against the signed exception log. The segmentation boundary is reviewed against the previous year's assessment. Testing covers the failure case, not only the happy path.

The email authentication record is compared with the most recent exercise record. The remote access path is reconciled with the quarterly review notes. The control is tested at least once every twelve months.

The awareness cycle is traced to the commissioning document. The segmentation boundary is evidenced by the current written standard. Metrics are reported as trends rather than single data points.

Each administrative account is measured against the register of exceptions. The physical controls is validated by the ticket history for the period. The segmentation boundary is evidenced by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The hardened build is documented alongside the ticket history for the period. The risk register is reconciled with the signed exception log. The encryption standard is evidenced by the quarterly review notes. Each administrative account is evidenced by the agreed service level. Third parties must demonstrate the control before access is granted.

The vendor register is documented alongside the commissioning document. The risk register is reconciled with the commissioning document. The cloud baseline is compared with the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is compared with the signed exception log. The awareness cycle is reviewed against the approved design baseline. The patch calendar is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The segmentation boundary is evidenced by the current written standard. The physical controls is documented alongside the quarterly review notes. The privileged access list is checked against the commissioning document. The continuity plan is documented alongside the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is validated by the evidence pack held by the owner. The classification scheme is checked against the evidence pack held by the owner. The backup rotation is validated by the commissioning document. The endpoint baseline is validated by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.