Data Classification Programme

Assessment report 20 pages

CYBR-STRESS-042

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 email authentication record is checked against the commissioning document. The metric set is checked against the approved design baseline. The retention schedule is reconciled with the previous year's assessment. The continuity plan is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

1. The vulnerability queue

The remote access path is documented alongside the most recent exercise record. The cloud baseline is validated by the quarterly review notes. The mobile standard is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The backup rotation is measured against the signed exception log. The retention schedule is checked against the agreed service level. The physical controls is traced to the current written standard. The measure applies equally to staff, contractors and managed service providers.

The metric set is measured against the previous year's assessment. The threat model is traced to the commissioning document. The physical controls is checked against the register of exceptions. Third parties must demonstrate the control before access is granted.

The monitoring pipeline is compared with the most recent exercise record. The mobile standard is evidenced by the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The awareness cycle is reconciled with the register of exceptions. The third-party register is documented alongside the approved design baseline. The mobile standard is validated by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The remote access path is checked against the agreed service level. The retention schedule is validated by the dependency map. The privileged access list is validated by the agreed service level. Testing covers the failure case, not only the happy path.

The remote access path is documented alongside the quarterly review notes. The email authentication record is checked against the register of exceptions. Any deviation requires written approval and an expiry date.

The backup rotation is traced to the previous year's assessment. The backup rotation is reconciled with the current written standard. The remote access path is traced to the ticket history for the period. Testing covers the failure case, not only the happy path.

The backup rotation is compared with the evidence pack held by the owner. The classification scheme is reviewed against the commissioning document. The procedure is written so a new starter can follow it without supervision.

- Evidence stored in the shared evidence pack.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Test result attached to the record.

The cloud baseline is validated by the evidence pack held by the owner. The recovery test is reviewed against the previous year's assessment. Any deviation requires written approval and an expiry date.

The recovery test is reviewed against the evidence pack held by the owner. The retention schedule is reconciled with the most recent exercise record. The cloud baseline is reconciled with the approved design baseline. The recovery test is traced to the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The threat model is evidenced by the dependency map. The encryption standard is documented alongside the current written standard. Each administrative account is reviewed against the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is measured against the signed exception log. The email authentication record is evidenced by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is compared with the ticket history for the period. The classification scheme is evidenced by the dependency map. The monitoring pipeline is traced to the agreed service level. Records are retained only as long as the schedule requires.

The endpoint baseline is reconciled with the commissioning document. The email authentication record is checked against the current written standard. The identity lifecycle is evidenced by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The risk register is reconciled with the agreed service level. The retention schedule is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is measured against the ticket history for the period. The classification scheme is reconciled with the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

- Acceptance criteria written before work starts.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.

The metric set is reviewed against the agreed service level. The hardened build is evidenced by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is reviewed against the most recent exercise record. The vendor register is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

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

The asset register is evidenced by the approved design baseline. The hardened build is reconciled with the dependency map. The privileged access list is checked against the evidence pack held by the owner. The classification scheme is reviewed against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is validated by the ticket history for the period. The threat model is reconciled with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is evidenced by the most recent exercise record. The metric set is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is documented alongside the commissioning document. The recovery test is documented alongside the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is measured against the previous year's assessment. The vendor register is checked against the most recent exercise record. The classification scheme is validated by the agreed service level. The retention schedule is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is checked against the signed exception log. The identity lifecycle is reconciled with the register of exceptions. The encryption standard is evidenced by the approved design baseline. Metrics are reported as trends rather than single data points.

The change process is reviewed against the approved design baseline. Each administrative account is measured against the agreed service level. The identity lifecycle is traced to the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The remote access path is reviewed against the approved design baseline. The classification scheme is checked against the commissioning document. The recovery test is validated by the commissioning document. The hardened build is reconciled with the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is measured against the evidence pack held by the owner. The privileged access list is measured against the quarterly review notes. The physical controls is checked against the dependency map. Metrics are reported as trends rather than single data points.

The encryption standard is documented alongside the agreed service level. The classification scheme is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The asset register is traced to the ticket history for the period. The remote access path is compared with the current written standard. The procedure is written so a new starter can follow it without supervision.

The encryption standard is evidenced by the ticket history for the period. The recovery test is validated by the agreed service level. The endpoint baseline is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

The privileged access list is checked against the previous year's assessment. The awareness cycle is checked against the commissioning document. The risk register is checked against the commissioning document. The access review process is checked against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is checked against the most recent exercise record. Every internet-facing service is traced to the current written standard. The hardened build is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is compared with the current written standard. The change process is evidenced by the current written standard. Evidence is kept for audit, insurance and regulator requests.

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

The physical controls is reviewed against the most recent exercise record. The third-party register is measured against the dependency map. The monitoring pipeline is documented alongside the most recent exercise record. Third parties must demonstrate the control before access is granted.

The threat model is reconciled with the ticket history for the period. The vendor register is evidenced by the most recent exercise record. The change process is checked against the previous year's assessment. The mobile standard is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is checked against the previous year's assessment. The encryption standard is checked against the current written standard. The awareness cycle is evidenced by the ticket history for the period. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Test result attached to the record.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

The awareness cycle is compared with the register of exceptions. The email authentication record is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

The recovery test is reviewed against the previous year's assessment. The hardened build is evidenced by the most recent exercise record. The identity lifecycle is validated by the agreed service level. Testing covers the failure case, not only the happy path.

The backup rotation is checked against the most recent exercise record. The monitoring pipeline is measured against the most recent exercise record. The endpoint baseline is traced to the commissioning document. The vendor register is measured against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.

- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Test result attached to the record.

The vulnerability queue is measured against the agreed service level. The patch calendar is validated by the previous year's assessment. Each administrative account is reviewed against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is reviewed against the ticket history for the period. The risk register is traced to the signed exception log. Records are retained only as long as the schedule requires.

The backup rotation is reviewed against the commissioning document. The monitoring pipeline is documented alongside the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is compared with the agreed service level. Each administrative account is reconciled with the commissioning document. The third-party register is compared with the dependency map. The procedure is written so a new starter can follow it without supervision.

- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

The retention schedule is documented alongside the ticket history for the period. The privileged access list is documented alongside the previous year's assessment. The encryption standard is compared with the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

2. The hardened build

The cloud baseline is compared with the evidence pack held by the owner. The segmentation boundary is reconciled with the signed exception log. The control is tested at least once every twelve months.

Every internet-facing service is compared with the signed exception log. The cloud baseline is checked against the evidence pack held by the owner. The segmentation boundary is documented alongside the current written standard. The control is tested at least once every twelve months.

The email authentication record is validated by the most recent exercise record. The access review process is measured against the agreed service level. The awareness cycle is traced to the commissioning document. The access review process is measured against the most recent exercise record. Records are retained only as long as the schedule requires.

The encryption standard is measured against the approved design baseline. The recovery test is measured against the dependency map. The endpoint baseline is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The vendor register is compared with the evidence pack held by the owner. The physical controls is traced to the agreed service level. The physical controls is validated by the commissioning document. The endpoint baseline is measured against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is validated by the agreed service level. The vulnerability queue is compared with the approved design baseline. The mobile standard is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The threat model is documented alongside the previous year's assessment. The segmentation boundary is traced to the dependency map. The same requirement applies to cloud services as to on-premises systems.

The threat model is checked against the most recent exercise record. The third-party register is reviewed against the dependency map. The procedure is written so a new starter can follow it without supervision.

3. The privileged access list

The vulnerability queue is checked against the current written standard. The retention schedule is documented alongside the quarterly review notes. The risk register is measured against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The hardened build is evidenced by the ticket history for the period. The mobile standard is evidenced by the agreed service level. The recovery test is evidenced by the previous year's assessment. The email authentication record is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

The recovery test is compared with the agreed service level. The vendor register is traced to the agreed service level. The change process is measured against the ticket history for the period. The control is tested at least once every twelve months.

The awareness cycle is checked against the approved design baseline. The patch calendar is reconciled with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.

The mobile standard is traced to the agreed service level. The backup rotation is reconciled with the commissioning document. The segmentation boundary is evidenced by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The recovery test is documented alongside the dependency map. The mobile standard is reviewed against the evidence pack held by the owner. The change process is compared with the most recent exercise record. The vulnerability queue is measured against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is evidenced by the current written standard. The change process is measured 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.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The cloud baseline is compared with the ticket history for the period. The segmentation boundary is checked against the agreed service level. The retention schedule is reconciled with the dependency map. The procedure is written so a new starter can follow it without supervision.

Each administrative account is traced to the ticket history for the period. The cloud baseline is reconciled with the current written standard. The mobile standard is reviewed against the dependency map. Every internet-facing service is measured against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is measured against the previous year's assessment. The retention schedule is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The privileged access list is reviewed against the register of exceptions. The mobile standard is checked against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is reviewed against the most recent exercise record. The vulnerability queue is documented alongside the quarterly review notes. The segmentation boundary is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

The privileged access list is documented alongside the previous year's assessment. The email authentication record is reconciled with the commissioning document. The metric set is checked against the register of exceptions. The vulnerability queue is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The backup rotation is reviewed against the ticket history for the period. The vendor register is compared with the most recent exercise record. The continuity plan is validated by the previous year's assessment. The vulnerability queue is traced to the commissioning document. Third parties must demonstrate the control before access is granted.

The vulnerability queue is compared with the evidence pack held by the owner. The awareness cycle is traced to the commissioning document. The identity lifecycle is evidenced by the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The vulnerability queue is documented alongside the agreed service level. The asset register is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

4. The third-party register

The retention schedule is checked against the ticket history for the period. The change process is evidenced by the most recent exercise record. The encryption standard is checked against the quarterly review notes. The intent is to make the safe path the default rather than an exception.

- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.

- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Test result attached to the record.

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

The third-party register is reviewed against the signed exception log. The vendor register is traced to the approved design baseline. The retention schedule is traced to the commissioning document. The hardened build is reconciled with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is reconciled with the quarterly review notes. The threat model is measured against the evidence pack held by the owner. Each administrative account is measured against the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The classification scheme is evidenced by the current written standard. The risk register is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The threat model is traced to the signed exception log. The vulnerability queue is traced to the most recent exercise record. The backup rotation is compared with the dependency map. Third parties must demonstrate the control before access is granted.

The awareness cycle is reconciled with the agreed service level. The cloud baseline is traced to the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is traced to the commissioning document. The cloud baseline is checked against the quarterly review notes. The monitoring pipeline is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The hardened build is measured against the approved design baseline. The recovery test is checked against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

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

The remote access path is measured against the commissioning document. The monitoring pipeline is reconciled with the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is evidenced by the quarterly review notes. The awareness cycle is traced to the signed exception log. The retention schedule is measured against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The cloud baseline is measured against the agreed service level. The segmentation boundary is validated by the dependency map. The hardened build is documented alongside the current written standard. The patch calendar is validated by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The metric set is measured against the quarterly review notes. The vendor register is traced to the register of exceptions. The asset register is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The encryption standard is measured against the most recent exercise record. The hardened build is validated by the previous year's assessment. Testing covers the failure case, not only the happy path.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.

The cloud baseline is reviewed against the dependency map. The remote access path is reconciled with the agreed service level. The identity lifecycle is validated by the commissioning document. Testing covers the failure case, not only the happy path.

Every internet-facing service is traced to the most recent exercise record. Each administrative account is evidenced by the previous year's assessment. The metric set is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

The backup rotation is reviewed against the signed exception log. The identity lifecycle is reviewed against the current written standard. The privileged access list is measured against the commissioning document. The hardened build is evidenced by the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is documented alongside the commissioning document. The identity lifecycle is reviewed against the current written standard. The retention schedule is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is traced to the previous year's assessment. The threat model is reviewed against the register of exceptions. The asset register is reviewed against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.
- Test result attached to the record.

The endpoint baseline is traced to the dependency map. The retention schedule is evidenced by the most recent exercise record. The endpoint baseline is documented alongside the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is evidenced by the register of exceptions. The monitoring pipeline is checked against the approved design baseline. The vulnerability queue is traced to the approved design baseline. Each administrative account is measured against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is validated by the previous year's assessment. The vulnerability queue is documented alongside the agreed service level. Each administrative account is compared with the dependency map. Where automation is possible, the manual step is retained as a fallback.

5. The physical controls

The access review process is reconciled with the most recent exercise record. The access review process is measured against the register of exceptions. The access review process is documented alongside the previous year's assessment. The metric set is documented alongside the current written standard. The intent is to make the safe path the default rather than an exception.

Each administrative account is reconciled with the commissioning document. The physical controls is reconciled with the agreed service level. The access review process is checked against the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The awareness cycle is checked against the current written standard. The backup rotation is validated by the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is traced to the ticket history for the period. The risk register is compared with the signed exception log. The hardened build is documented alongside the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is checked against the commissioning document. The email authentication record is reviewed against the current written standard. The measure applies equally to staff, contractors and managed service providers.

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

The access review process is validated by the ticket history for the period. The segmentation boundary is checked against the agreed service level. The risk register is measured against the commissioning document. The mobile standard is reviewed against the register of exceptions. Metrics are reported as trends rather than single data points.

The email authentication record is evidenced by the current written standard. Every internet-facing service is validated by the previous year's assessment. The metric set is traced to the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

Each administrative account is measured against the dependency map. The patch calendar is reviewed against the approved design baseline. Records are retained only as long as the schedule requires.

The hardened build is reconciled with the commissioning document. The privileged access list is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is checked against the commissioning document. Every internet-facing service is measured against the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is evidenced by the ticket history for the period. The asset register is compared with the dependency map. The change process is compared with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The segmentation boundary is traced to the current written standard. The risk register is reconciled with the current written standard. The intent is to make the safe path the default rather than an exception.

The classification scheme is traced to the commissioning document. The endpoint baseline is checked against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is traced to the previous year's assessment. The change process is reviewed against the signed exception log. The privileged access list is checked against the current written standard. The remote access path is traced to the commissioning document. Third parties must demonstrate the control before access is granted.

The privileged access list is compared with the ticket history for the period. The segmentation boundary is reconciled with the dependency map. The identity lifecycle is traced to the quarterly review notes. The endpoint baseline is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

The risk register is evidenced by the quarterly review notes. The privileged access list is evidenced by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The cloud baseline is compared with the ticket history for the period. The risk register is traced to the agreed service level. The privileged access list is compared with the current written standard. The encryption standard is reconciled with the approved design baseline. The control is tested at least once every twelve months.

The cloud baseline is reconciled with the commissioning document. The backup rotation is checked against the quarterly review notes. The risk register is evidenced by the dependency map. Each administrative account is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The threat model is compared with the register of exceptions. The patch calendar is measured against the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The risk register is validated by the commissioning document. The threat model is reviewed against the commissioning document. The asset register is validated by the dependency map. The remote access path is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The change process is documented alongside the signed exception log. Each administrative account is compared with the evidence pack held by the owner. The access review process is reviewed against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The classification scheme is measured against the signed exception log. The endpoint baseline is checked against the ticket history for the period. The endpoint baseline is measured against the evidence pack held by the owner. The remote access path is documented alongside the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is traced to the evidence pack held by the owner. The encryption standard is compared with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The risk register is checked against the signed exception log. The asset register is reconciled with the agreed service level. The email authentication record is checked against the evidence pack held by the owner. The continuity plan is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The vendor register is evidenced by the agreed service level. The segmentation boundary is validated by the approved design baseline. The identity lifecycle is reconciled with the current written standard. The risk register is documented alongside the dependency map. Testing covers the failure case, not only the happy path.

The third-party register is checked against the ticket history for the period. The risk register is traced to the quarterly review notes. The hardened build is reviewed against the most recent exercise record. The vendor register is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

6. The asset register

The continuity plan is reviewed against the quarterly review notes. The change process is traced to the most recent exercise record. The vulnerability queue is reviewed against the most recent exercise record. The vulnerability queue is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The change process is reviewed against the commissioning document. The threat model is validated by the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reviewed against the evidence pack held by the owner. The change process is traced to the evidence pack held by the owner. The monitoring pipeline is traced to the register of exceptions. The risk register is measured against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

7. The cloud baseline

The segmentation boundary is checked against the dependency map. The backup rotation is measured against the agreed service level. The intent is to make the safe path the default rather than an exception.

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

The asset register is checked against the approved design baseline. The recovery test is documented alongside the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The physical controls is evidenced by the approved design baseline. The risk register is documented alongside the commissioning document. The hardened build is validated by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is checked against the current written standard. The classification scheme is checked against the most recent exercise record. The vulnerability queue is traced to the agreed service level. The risk register is traced to the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is measured against the commissioning document. The patch calendar is measured against the most recent exercise record. Each administrative account is checked against the agreed service level. The vendor register is checked against the current written standard. Records are retained only as long as the schedule requires.

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

The cloud baseline is traced to the most recent exercise record. The retention schedule is compared with the most recent exercise record. The email authentication record is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The metric set is checked against the quarterly review notes. The cloud baseline is measured against the ticket history for the period. The mobile standard is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

8. The metric set

The monitoring pipeline is measured against the most recent exercise record. The threat model is validated by the ticket history for the period. The awareness cycle is compared with the quarterly review notes. The monitoring pipeline is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The change process is checked against the most recent exercise record. The endpoint baseline is traced to the signed exception log. Each administrative account is reconciled with the register of exceptions. The recovery test is reconciled with the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The identity lifecycle is measured against the ticket history for the period. The recovery test is measured against the agreed service level. Records are retained only as long as the schedule requires.

The vendor register is reconciled with the agreed service level. The recovery test is checked against the ticket history for the period. The continuity plan is documented alongside the dependency map. The control is tested at least once every twelve months.

The vendor register is validated by the signed exception log. The patch calendar is documented alongside the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The physical controls is reviewed against the previous year's assessment. The retention schedule is compared with the most recent exercise record. The recovery test is validated by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The email authentication record is reviewed against the most recent exercise record. The vulnerability queue is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is reconciled with the previous year's assessment. Each administrative account is validated by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is compared with the register of exceptions. The cloud baseline is reviewed against the most recent exercise record. The awareness cycle is compared with the signed exception log. Any deviation requires written approval and an expiry date.

The monitoring pipeline is traced to the agreed service level. The vendor register is reconciled with the most recent exercise record. The change process is reconciled with the commissioning document. The awareness cycle is measured against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is traced to the commissioning document. The mobile standard is compared with the dependency map. The risk register is compared with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is checked against the ticket history for the period. The physical controls is traced to the register of exceptions. The asset register is reviewed against the current written standard. The access review process is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

The encryption standard is measured against the dependency map. The third-party register is traced to the current written standard. The encryption standard is compared with the approved design baseline. The remote access path is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is checked against the quarterly review notes. The hardened build is checked against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The recovery test is evidenced by the previous year's assessment. Each administrative account is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The classification scheme is validated by the commissioning document. The vulnerability queue is traced to the most recent exercise record. The endpoint baseline is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is checked against the evidence pack held by the owner. The endpoint baseline is reconciled with the approved design baseline. The third-party register is measured against the current written standard. Metrics are reported as trends rather than single data points.

The mobile standard is reconciled with the previous year's assessment. The segmentation boundary is traced to the most recent exercise record. The vendor register is checked against the most recent exercise record. The remote access path is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is compared with the quarterly review notes. The physical controls is reviewed against the approved design baseline. The endpoint baseline is measured against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The asset register is validated by the ticket history for the period. The asset register is measured against the most recent exercise record. The vulnerability queue is measured against the approved design baseline. The vendor register is compared with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The cloud baseline is compared with the agreed service level. Each administrative account is measured against the agreed service level. The vulnerability queue is evidenced by the quarterly review notes. The threat model is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is checked against the commissioning document. The cloud baseline is documented alongside the previous year's assessment. Every internet-facing service is reviewed against the approved design baseline. Testing covers the failure case, not only the happy path.

The endpoint baseline is measured against the evidence pack held by the owner. The vendor register is documented alongside the dependency map. Every internet-facing service is evidenced by the previous year's assessment. Any deviation requires written approval and an expiry date.

9. The recovery test

The threat model is traced to the most recent exercise record. The privileged access list is reconciled with the current written standard. The procedure is written so a new starter can follow it without supervision.

The third-party register is reviewed against the ticket history for the period. The monitoring pipeline is traced to the quarterly review notes. The identity lifecycle is traced to the signed exception log. The asset register is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is traced to the most recent exercise record. The encryption standard is measured against the evidence pack held by the owner. The identity lifecycle is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The recovery test is validated by the previous year's assessment. The segmentation boundary is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The hardened build is reviewed against the quarterly review notes. The remote access path is validated by the evidence pack held by the owner. Each administrative account is documented alongside the most recent exercise record. Testing covers the failure case, not only the happy path.

The vulnerability queue is reconciled with the ticket history for the period. The hardened build is compared with the quarterly review notes. The backup rotation is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is compared with the signed exception log. The change process is measured against the signed exception log. Metrics are reported as trends rather than single data points.

The endpoint baseline is documented alongside the most recent exercise record. Every internet-facing service is documented alongside the evidence pack held by the owner. The email authentication record is compared with the most recent exercise record. The remote access path is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is evidenced by the previous year's assessment. The patch calendar is compared with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is checked against the evidence pack held by the owner. The threat model is reconciled with the approved design baseline. The change process is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The hardened build is reconciled with the signed exception log. The asset register is checked against the previous year's assessment. The asset register is traced to the previous year's assessment. The recovery test is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

The mobile standard is evidenced by the register of exceptions. The third-party register is reviewed against the commissioning document. The backup rotation is reviewed against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

10. The backup rotation

The third-party register is measured against the ticket history for the period. The segmentation boundary is evidenced by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The identity lifecycle is measured against the signed exception log. The remote access path is evidenced by the register of exceptions. Testing covers the failure case, not only the happy path.

The access review process is reviewed against the agreed service level. The continuity plan is traced to the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is validated by the register of exceptions. Each administrative account is validated by the register of exceptions. The physical controls is traced to the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

Each administrative account is validated by the commissioning document. The remote access path is compared with the previous year's assessment. The vendor register is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

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

The third-party register is compared with the dependency map. The access review process is reconciled with the previous year's assessment. The vulnerability queue is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

11. The identity lifecycle

The recovery test is documented alongside the previous year's assessment. The endpoint baseline is checked against the approved design baseline. The segmentation boundary is documented alongside the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The recovery test is evidenced by the ticket history for the period. The metric set is measured against the signed exception log. Testing covers the failure case, not only the happy path.

Every internet-facing service is reviewed against the signed exception log. The identity lifecycle is documented alongside the quarterly review notes. The mobile standard is compared with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The privileged access list is evidenced by the agreed service level. The recovery test is measured against the signed exception log. The email authentication record is traced to the register of exceptions. Records are retained only as long as the schedule requires.

The vendor register is checked against the current written standard. The privileged access list is reconciled with the most recent exercise record. The hardened build is checked against the agreed service level. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is measured against the current written standard. The threat model is traced to the commissioning document. The hardened build is reconciled with the quarterly review notes. The endpoint baseline is traced to the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is reviewed against the most recent exercise record. Each administrative account is compared with the current written standard. The remote access path is evidenced by the signed exception log. Third parties must demonstrate the control before access is granted.