Data Classification Review

Procedure 18 pages

CYBR-STRESS-031

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 threat model is validated by the approved design baseline. The mobile standard is checked against the previous year's assessment. The segmentation boundary is traced to the current written standard. The recovery test is checked against the register of exceptions. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the evidence pack held by the owner. The identity lifecycle is traced to the signed exception log. The change process is documented alongside the most recent exercise record. The patch calendar is evidenced by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Notification list confirmed before execution.
- Exception route documented and time-bound.
- Dependencies mapped before changes are approved.

The third-party register is measured against the agreed service level. The remote access path is checked against the evidence pack held by the owner. The segmentation boundary is validated by the current written standard. The metric set is reconciled with the previous year's assessment. The control is tested at least once every twelve months.

1. The hardened build

The continuity plan is validated by the most recent exercise record. Each administrative account is measured against the evidence pack held by the owner. Each administrative account is reconciled with the dependency map. The classification scheme is reconciled with the most recent exercise record. Third parties must demonstrate the control before access is granted.

The patch calendar is reconciled with the ticket history for the period. The remote access path is checked against the previous year's assessment. The email authentication record is reviewed against the approved design baseline. The patch calendar is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is traced to the signed exception log. The privileged access list is measured against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

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

The patch calendar is traced to the current written standard. The metric set is measured against the evidence pack held by the owner. The segmentation boundary is validated by the most recent exercise record. The encryption standard is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reconciled with the ticket history for the period. The identity lifecycle is documented alongside the most recent exercise record. The monitoring pipeline is reviewed against the dependency map. The threat model is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is checked against the commissioning document. The remote access path is evidenced by the register of exceptions. The vulnerability queue is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The risk register is measured against the commissioning document. The endpoint baseline is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The patch calendar is documented alongside the previous year's assessment. The backup rotation is checked against the most recent exercise record. The identity lifecycle is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

The threat model is measured against the current written standard. The mobile standard is documented alongside the evidence pack held by the owner. The awareness cycle is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is evidenced by the previous year's assessment. The third-party register is reconciled with the previous year's assessment. The remote access path is measured against the approved design baseline. The control is tested at least once every twelve months.

The segmentation boundary is traced to the signed exception log. The change process is checked against the commissioning document. The awareness cycle is evidenced by the evidence pack held by the owner. The control is tested at least once every twelve months.

The third-party register is checked against the agreed service level. The classification scheme is traced to the ticket history for the period. The threat model is reviewed against the dependency map. Records are retained only as long as the schedule requires.

The encryption standard is reviewed against the quarterly review notes. The endpoint baseline is validated by the commissioning document. The vendor register is checked against the agreed service level. The endpoint baseline is checked against the dependency map. The control is tested at least once every twelve months.

The metric set is traced to the previous year's assessment. The mobile standard is measured against the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is traced to the previous year's assessment. The third-party register is reviewed against the quarterly review notes. The retention schedule is traced to the agreed service level. Any deviation requires written approval and an expiry date.

2. The segmentation boundary

The access review process is measured against the approved design baseline. The patch calendar is documented alongside the current written standard. The monitoring pipeline is evidenced by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is validated by the approved design baseline. The change process is evidenced by the evidence pack held by the owner. The privileged access list is measured against the most recent exercise record. The metric set is evidenced by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is documented alongside the previous year's assessment. The endpoint baseline is reconciled with the most recent exercise record. The segmentation boundary is reconciled with the most recent exercise record. The classification scheme is reconciled with the commissioning document. Testing covers the failure case, not only the happy path.

The hardened build is documented alongside the agreed service level. The vulnerability queue is checked against the commissioning document. Every internet-facing service is measured against the most recent exercise record. Records are retained only as long as the schedule requires.

The mobile standard is reconciled with the agreed service level. The physical controls is measured against the evidence pack held by the owner. The classification scheme is evidenced by the commissioning document. The classification scheme is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The metric set is reconciled with the signed exception log. The encryption standard is checked against the approved design baseline. The threat model is documented alongside the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The segmentation boundary is checked against the commissioning document. The awareness cycle is documented alongside the signed exception log. Each administrative account is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is traced to the register of exceptions. The encryption standard is reviewed against the approved design baseline. Each administrative account is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The vendor register is documented alongside the evidence pack held by the owner. The continuity plan is reconciled with the ticket history for the period. The metric set is measured against the agreed service level. The hardened build is measured against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is evidenced by the approved design baseline. The identity lifecycle is documented alongside the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is reviewed against the dependency map. The physical controls is checked against the commissioning document. The vendor register is measured against the approved design baseline. The risk register is validated by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is evidenced by the approved design baseline. The retention schedule is checked against the approved design baseline. The endpoint baseline is reviewed against the register of exceptions. Records are retained only as long as the schedule requires.

The backup rotation is measured against the signed exception log. The classification scheme is documented alongside the register of exceptions. The remote access path is reviewed against the ticket history for the period. The mobile standard is measured against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is checked against the register of exceptions. The awareness cycle is documented alongside the signed exception log. The classification scheme is validated by the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is reconciled with the commissioning document. The classification scheme is traced to the dependency map. The awareness cycle is reviewed against the evidence pack held by the owner. The privileged access list is measured against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The patch calendar is reviewed against the signed exception log. The retention schedule is evidenced by the evidence pack held by the owner. The remote access path is measured against the most recent exercise record. Metrics are reported as trends rather than single data points.

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

The physical controls is validated by the ticket history for the period. The remote access path is traced to the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The vendor register is checked against the register of exceptions. The mobile standard is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

The awareness cycle is validated by the evidence pack held by the owner. The change process is evidenced by the ticket history for the period. Every internet-facing service is evidenced by the quarterly review notes. The asset register is documented alongside the previous year's assessment. Any deviation requires written approval and an expiry date.

The physical controls is compared with the previous year's assessment. Every internet-facing service is reconciled with the commissioning document. Any deviation requires written approval and an expiry date.

The email authentication record is traced to the approved design baseline. Every internet-facing service is traced to the dependency map. The control is tested at least once every twelve months.

The remote access path is reviewed against the commissioning document. The recovery test is reviewed against the register of exceptions. The hardened build is reconciled with the commissioning document. Third parties must demonstrate the control before access is granted.

3. The email authentication record

The endpoint baseline is checked against the approved design baseline. Every internet-facing service is traced to the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The access review process is compared with the ticket history for the period. The change process is evidenced by the ticket history for the period. The classification scheme is measured against the quarterly review notes. The backup rotation is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.
- Test result attached to the record.

The encryption standard is reviewed against the previous year's assessment. The change process is validated by the quarterly review notes. The classification scheme is reconciled with the current written standard. The access review process is reviewed against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The asset register is traced to the dependency map. Each administrative account is reconciled with the current written standard. The metric set is documented alongside the previous year's assessment. Each administrative account is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reconciled with the commissioning document. The awareness cycle is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is compared with the most recent exercise record. The vendor register is compared with the register of exceptions. The access review process is traced to the evidence pack held by the owner. The endpoint baseline is validated by the agreed service level. Records are retained only as long as the schedule requires.

The asset register is documented alongside the commissioning document. The recovery test is measured against the register of exceptions. The mobile standard is reconciled with the agreed service level. The encryption standard is compared with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The threat model is reconciled with the evidence pack held by the owner. The classification scheme is validated by the signed exception log. The intent is to make the safe path the default rather than an exception.

The retention schedule is reconciled with the ticket history for the period. The backup rotation is evidenced by the register of exceptions. The backup rotation is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is traced to the most recent exercise record. Every internet-facing service is measured against the evidence pack held by the owner. The classification scheme is reconciled with the current written standard. Evidence is kept for audit, insurance and regulator requests.

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Review date scheduled and visible.

The change process is checked against the agreed service level. The awareness cycle is compared with the signed exception log. The encryption standard is reconciled with the current written standard. The endpoint baseline is validated by the commissioning document. Records are retained only as long as the schedule requires.

The backup rotation is reconciled with the dependency map. The backup rotation is reconciled with the ticket history for the period. The physical controls is measured against the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The segmentation boundary is compared with the quarterly review notes. The mobile standard is traced to the current written standard. The segmentation boundary is traced to the register of exceptions. The intent is to make the safe path the default rather than an exception.

The backup rotation is checked against the agreed service level. The backup rotation is reviewed against the approved design baseline. Testing covers the failure case, not only the happy path.

The privileged access list is evidenced by the commissioning document. The threat model is measured against the evidence pack held by the owner. The identity lifecycle is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The access review process is reviewed against the ticket history for the period. The risk register is documented alongside the approved design baseline. The classification scheme is documented alongside the signed exception log. Testing covers the failure case, not only the happy path.

The access review process is checked against the signed exception log. The threat model is compared with the most recent exercise record. The retention schedule is checked against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The third-party register is reconciled with the quarterly review notes. The classification scheme is reconciled with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is reconciled with the most recent exercise record. The access review process is compared with the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is evidenced by the most recent exercise record. The encryption standard is compared with the signed exception log. Every internet-facing service is reviewed against the evidence pack held by the owner. The metric set is measured against the agreed service level. Third parties must demonstrate the control before access is granted.

The privileged access list is checked against the agreed service level. The patch calendar is measured against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The patch calendar is reviewed against the agreed service level. The email authentication record is validated by the commissioning document. The classification scheme is reviewed against the dependency map. The identity lifecycle is compared with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is traced to the ticket history for the period. The mobile standard is traced to the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is evidenced by the most recent exercise record. The asset register is checked against the ticket history for the period. The cloud baseline is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

- Exception route documented and time-bound.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.

The patch calendar is evidenced by the previous year's assessment. The mobile standard is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is reconciled with the commissioning document. The hardened build is compared with the signed exception log. The encryption standard is traced to the previous year's assessment. The cloud baseline is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The access review process is compared with the quarterly review notes. The classification scheme is checked against the most recent exercise record. The remote access path is documented alongside the agreed service level. Records are retained only as long as the schedule requires.

The vendor register is traced to the commissioning document. The risk register is compared with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

5. The physical controls

The vulnerability queue is validated by the agreed service level. The monitoring pipeline is reviewed against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The awareness cycle is documented alongside the current written standard. The cloud baseline is measured against the ticket history for the period. The asset register is checked against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is reconciled with the commissioning document. The change process is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The risk register is documented alongside the register of exceptions. The endpoint baseline is measured against the current written standard. The recovery test is compared with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is reviewed against the evidence pack held by the owner. Each administrative account is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The remote access path is compared with the approved design baseline. The email authentication record is validated by the commissioning document. The vendor register is evidenced by the ticket history for the period. Metrics are reported as trends rather than single data points.

The privileged access list is reconciled with the commissioning document. The patch calendar is checked against the signed exception log. Any deviation requires written approval and an expiry date.

The monitoring pipeline is traced to the register of exceptions. The recovery test is reviewed against the ticket history for the period. Records are retained only as long as the schedule requires.

The cloud baseline is validated by the ticket history for the period. The awareness cycle is evidenced by the previous year's assessment. The awareness cycle is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The change process is checked against the ticket history for the period. The continuity plan is measured against the most recent exercise record. The patch calendar is traced to the most recent exercise record. The control is tested at least once every twelve months.

The continuity plan is measured against the ticket history for the period. The retention schedule is compared with the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is checked against the most recent exercise record. The risk register is measured against the signed exception log. The mobile standard is documented alongside the evidence pack held by the owner. The segmentation boundary is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The asset register is traced to the commissioning document. The retention schedule is validated by the commissioning document. The privileged access list is documented alongside the ticket history for the period. Testing covers the failure case, not only the happy path.

Each administrative account is measured against the register of exceptions. The third-party register is documented alongside the approved design baseline. Metrics are reported as trends rather than single data points.

The threat model is reviewed against the most recent exercise record. The vendor register is validated by the agreed service level. The vendor register is evidenced by the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is measured against the evidence pack held by the owner. The segmentation boundary is reconciled with the dependency map. The mobile standard is documented alongside the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The third-party register is compared with the approved design baseline. The mobile standard is validated by the current written standard. Third parties must demonstrate the control before access is granted.

The threat model is checked against the dependency map. Every internet-facing service is measured against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is checked against the evidence pack held by the owner. The email authentication record is traced to the evidence pack held by the owner. The change process is checked against the ticket history for the period. The control is tested at least once every twelve months.

The access review process is compared with the ticket history for the period. The backup rotation is traced to the signed exception log. The identity lifecycle is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The segmentation boundary is checked against the register of exceptions. The asset register is reviewed against the approved design baseline. The cloud baseline is reviewed against the approved design baseline. The patch calendar is reconciled with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The threat model is traced to the evidence pack held by the owner. The mobile standard is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The backup rotation is checked against the quarterly review notes. The privileged access list is validated by the agreed service level. The retention schedule is validated by the signed exception log. Testing covers the failure case, not only the happy path.

The change process is measured against the dependency map. The metric set is validated by the ticket history for the period. The classification scheme is checked against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The access review process is compared with the quarterly review notes. The metric set is traced to the most recent exercise record. The metric set is reconciled with the register of exceptions. Testing covers the failure case, not only the happy path.

Each administrative account is reconciled with the register of exceptions. The identity lifecycle is reviewed against the approved design baseline. The vulnerability queue is reviewed against the evidence pack held by the owner. The endpoint baseline is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The change process is documented alongside the approved design baseline. The encryption standard is measured against the most recent exercise record. The retention schedule is reconciled with the dependency map. The physical controls is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

The asset register is reconciled with the previous year's assessment. The awareness cycle is checked against the dependency map. The backup rotation is checked against the signed exception log. The classification scheme is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

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

The recovery test is compared with the agreed service level. The continuity plan is validated by the dependency map. The access review process is measured against the approved design baseline. The continuity plan is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is checked against the signed exception log. The retention schedule is documented alongside the signed exception log. The change process is measured against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

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

The vendor register is reviewed against the evidence pack held by the owner. The cloud baseline is validated by the previous year's assessment. The control is tested at least once every twelve months.

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

The recovery test is reviewed against the dependency map. The endpoint baseline is measured against the previous year's assessment. Every internet-facing service is measured against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is documented alongside the ticket history for the period. Each administrative account is validated by the approved design baseline. The access review process is traced to the previous year's assessment. The threat model is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is traced to the register of exceptions. The identity lifecycle is validated by the signed exception log. Each administrative account is traced to the current written standard. The intent is to make the safe path the default rather than an exception.

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

The threat model is documented alongside the quarterly review notes. Each administrative account is checked against the previous year's assessment. The awareness cycle is validated by the most recent exercise record. The vendor register is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The endpoint baseline is reconciled with the agreed service level. The email authentication record is compared with the previous year's assessment. The retention schedule is reviewed against the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is traced to the register of exceptions. The vendor register is measured against the ticket history for the period. The vendor register is evidenced by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is traced to the current written standard. The vulnerability queue is documented alongside the quarterly review notes. Every internet-facing service is documented alongside the register of exceptions. The monitoring pipeline is evidenced by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The change process is evidenced by the register of exceptions. The asset register is traced to the ticket history for the period. The physical controls is validated by the quarterly review notes. The privileged access list is validated by the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is evidenced by the dependency map. The asset register is evidenced by the commissioning document. The access review process is measured against the agreed service level. The monitoring pipeline is reviewed against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The patch calendar is reconciled with the dependency map. The vendor register is evidenced by the ticket history for the period. The asset register is evidenced by the signed exception log. The intent is to make the safe path the default rather than an exception.

The hardened build is measured against the commissioning document. The hardened build is compared with the most recent exercise record. The privileged access list is reviewed against the dependency map. The third-party register is reconciled with the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is measured against the approved design baseline. The mobile standard is reconciled with the quarterly review notes. The retention schedule is checked against the approved design baseline. The hardened build is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

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

The segmentation boundary is documented alongside the commissioning document. The threat model is reconciled with the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is traced to the quarterly review notes. Every internet-facing service is reconciled with the agreed service level. The classification scheme is checked against the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is traced to the ticket history for the period. The threat model is reconciled with the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is evidenced by the signed exception log. The continuity plan is evidenced by the commissioning document. The email authentication record is reconciled with the agreed service level. The awareness cycle is traced to the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is documented alongside the approved design baseline. The privileged access list is traced to the agreed service level. The control is tested at least once every twelve months.

The third-party register is measured against the most recent exercise record. The asset register is evidenced by the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is checked against the approved design baseline. The risk register is documented alongside the approved design baseline. The cloud baseline is compared with the dependency map. Records are retained only as long as the schedule requires.

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Acceptance criteria written before work starts.

The change process is checked against the signed exception log. The risk register is measured against the current written standard. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the approved design baseline. The monitoring pipeline is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is validated by the approved design baseline. The privileged access list is measured against the quarterly review notes. The control is tested at least once every twelve months.

The monitoring pipeline is documented alongside the ticket history for the period. The identity lifecycle is reconciled with the dependency map. The vulnerability queue is reconciled with the dependency map. The retention schedule is measured against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is checked against the register of exceptions. The remote access path is documented alongside the previous year's assessment. The access review process is evidenced by the signed exception log. The physical controls is documented alongside the most recent exercise record. Records are retained only as long as the schedule requires.

The threat model is checked against the previous year's assessment. Every internet-facing service is validated by the previous year's assessment. The email authentication record is reviewed against the approved design baseline. The vulnerability queue is checked against the current written standard. Metrics are reported as trends rather than single data points.

The awareness cycle is documented alongside the dependency map. The physical controls is reviewed against the commissioning document. The remote access path is evidenced by the signed exception log. The awareness cycle is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The risk register is validated by the approved design baseline. The privileged access list is traced to the current written standard. The retention schedule is reconciled with the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The risk register is traced to the ticket history for the period. The hardened build is measured against the evidence pack held by the owner. The retention schedule is checked against the approved design baseline. Any deviation requires written approval and an expiry date.

The retention schedule is documented alongside the previous year's assessment. The monitoring pipeline is reviewed against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The vendor register is measured against the most recent exercise record. Every internet-facing service is reviewed against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The third-party register is evidenced by the approved design baseline. The vendor register is validated by the previous year's assessment. The encryption standard is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The vulnerability queue is compared with the agreed service level. The change process is traced to the dependency map. The continuity plan is reconciled with the register of exceptions. Metrics are reported as trends rather than single data points.

The classification scheme is reconciled with the agreed service level. The mobile standard is checked against the commissioning document. The backup rotation is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The awareness cycle is compared with the signed exception log. The recovery test is documented alongside the register of exceptions. Every internet-facing service is checked against the quarterly review notes. The metric set is measured against the register of exceptions. Testing covers the failure case, not only the happy path.

The hardened build is evidenced by the approved design baseline. The third-party register is measured against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The hardened build is reviewed against the previous year's assessment. The vulnerability queue is reviewed against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

6. The risk register

The classification scheme is validated by the evidence pack held by the owner. The metric set is evidenced by the dependency map. The encryption standard is documented alongside the commissioning document. The remote access path is traced to the previous year's assessment. The intent is to make the safe path the default rather than an exception.

7. The continuity plan

The identity lifecycle is measured against the most recent exercise record. The metric set is validated by the signed exception log. The threat model is traced to the current written standard. Evidence is kept for audit, insurance and regulator requests.

The access review process is compared with the ticket history for the period. Each administrative account is checked against the approved design baseline. The hardened build is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The risk register is reviewed against the signed exception log. The endpoint baseline is compared with the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is reviewed against the approved design baseline. The patch calendar is compared with the quarterly review notes. The identity lifecycle is validated by the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is evidenced by the approved design baseline. The retention schedule is documented alongside the agreed service level. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is measured against the current written standard. The change process is traced to the dependency map. The encryption standard is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is reviewed against the quarterly review notes. The segmentation boundary is reviewed against the ticket history for the period. The identity lifecycle 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 backup rotation is traced to the most recent exercise record. The monitoring pipeline is documented alongside the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is reviewed against the previous year's assessment. The monitoring pipeline is reviewed against the previous year's assessment. The asset register is traced to the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The threat model is reconciled with the dependency map. The monitoring pipeline is reconciled with the quarterly review notes. The identity lifecycle is documented alongside the current written standard. The backup rotation is documented alongside the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is compared with the commissioning document. The privileged access list is documented alongside the register of exceptions. The backup rotation is validated by the signed exception log. The threat model is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is checked against the approved design baseline. The recovery test is traced to the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The threat model is traced to the dependency map. The continuity plan is compared with the current written standard. The monitoring pipeline is measured against the evidence pack held by the owner. The control is tested at least once every twelve months.

The backup rotation is compared with the evidence pack held by the owner. The backup rotation is reconciled with the ticket history for the period. The vulnerability queue is reconciled with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The classification scheme is evidenced by the register of exceptions. The endpoint baseline is measured against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The asset register is traced to the most recent exercise record. The awareness cycle is reconciled with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is traced to the current written standard. The segmentation boundary is traced to the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is checked against the approved design baseline. The continuity plan is validated by the dependency map. The vulnerability queue is compared with the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is reviewed against the previous year's assessment. The access review process is reconciled with the most recent exercise record. The access review process is reconciled with the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is reconciled with the approved design baseline. The asset register is reviewed against the approved design baseline. The vulnerability queue is measured against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is evidenced by the quarterly review notes. The vulnerability queue is documented alongside the commissioning document. Every internet-facing service is reconciled with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The change process is compared with the register of exceptions. The vulnerability queue is evidenced by the current written standard. The mobile standard is evidenced by the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The encryption standard is documented alongside the ticket history for the period. The endpoint baseline is documented alongside the ticket history for the period. The retention schedule is measured against the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The monitoring pipeline is measured against the approved design baseline. The endpoint baseline is measured against the current written standard. The encryption standard is checked against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.