# Data Classification Baseline

Standards document  16 pages

CYBR-STRESS-043

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 mobile standard is measured against the register of exceptions. The privileged access list is validated by the previous year's assessment. The control is tested at least once every twelve months.

The change process is compared with the agreed service level. The endpoint baseline is checked against the quarterly review notes. The encryption standard is traced to the signed exception log. The risk register is evidenced by the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is evidenced by the commissioning document. The identity lifecycle is evidenced by the commissioning document. The remote access path is reviewed against the ticket history for the period. Any deviation requires written approval and an expiry date.

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

The backup rotation is measured against the quarterly review notes. The access review process is evidenced by the approved design baseline. The hardened build is traced to the ticket history for the period. Any deviation requires written approval and an expiry date.

The vendor register is checked against the register of exceptions. The vulnerability queue is evidenced by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The vendor register is reconciled with the previous year's assessment. The third-party register is traced to the signed exception log. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is validated by the agreed service level. The remote access path is reconciled with the ticket history for the period. Every internet-facing service is validated by the commissioning document. The awareness cycle is traced to the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The change process is measured against the approved design baseline. The recovery test is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The endpoint baseline is compared with the signed exception log. The patch calendar is documented alongside the quarterly review notes. The cloud baseline is reviewed against the register of exceptions. Metrics are reported as trends rather than single data points.

The risk register is compared with the current written standard. The third-party register is documented alongside the previous year's assessment. The identity lifecycle is checked against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is evidenced by the approved design baseline. The monitoring pipeline is compared with the agreed service level. Records are retained only as long as the schedule requires.

The endpoint baseline is measured against the dependency map. The recovery test is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The backup rotation is reconciled with the quarterly review notes. The backup rotation is measured against the previous year's assessment. Each administrative account is measured against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The risk register is checked against the ticket history for the period. The monitoring pipeline is reconciled with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The recovery test is reviewed against the quarterly review notes. The change process is validated by the commissioning document. The continuity plan is measured against the current written standard. The intent is to make the safe path the default rather than an exception.

The physical controls is validated by the quarterly review notes. The patch calendar is evidenced by the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The email authentication record is validated by the dependency map. The backup rotation is evidenced by the evidence pack held by the owner. The metric set is measured against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

## 2. The asset register

The third-party register is validated by the approved design baseline. The vendor register is validated by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is measured against the previous year's assessment. The change process is compared with the current written standard. Testing covers the failure case, not only the happy path.

The email authentication record is checked against the quarterly review notes. The endpoint baseline is documented alongside the ticket history for the period. Metrics are reported as trends rather than single data points.

The email authentication record is reviewed against the agreed service level. The identity lifecycle is reviewed against the evidence pack held by the owner. The retention schedule is evidenced by the current written standard. The privileged access list is reconciled with the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The continuity plan is documented alongside the agreed service level. The risk register is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The third-party register is traced to the quarterly review notes. The continuity plan is measured against the ticket history for the period. The continuity plan is reviewed against the most recent exercise record. The continuity plan is validated by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The threat model is compared with the approved design baseline. The recovery test is compared with the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The segmentation boundary is reconciled with the ticket history for the period. Each administrative account is compared with the ticket history for the period. The awareness cycle is validated by the register of exceptions. The third-party register is evidenced by the ticket history for the period. Testing covers the failure case, not only the happy path.

The vulnerability queue is measured against the evidence pack held by the owner. The classification scheme is validated by the evidence pack held by the owner. The identity lifecycle is reviewed against the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The recovery test is evidenced by the quarterly review notes. The awareness cycle is traced to the commissioning document. The awareness cycle is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The asset register is evidenced by the agreed service level. The backup rotation is traced to the dependency map. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is traced to the quarterly review notes. The segmentation boundary is checked against the quarterly review notes. The monitoring pipeline is reconciled with the commissioning document. The continuity plan is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

The backup rotation is validated by the signed exception log. The backup rotation is validated by the dependency map. The classification scheme is checked against the evidence pack held by the owner. The asset register is compared with the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

The privileged access list is reviewed against the dependency map. The vulnerability queue is measured against the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The hardened build is measured against the agreed service level. The identity lifecycle is measured against the signed exception log. The retention schedule is evidenced by the register of exceptions. The privileged access list is reviewed against the most recent exercise record. Records are retained only as long as the schedule requires.

The change process is compared with the quarterly review notes. The continuity plan is reconciled with the register of exceptions. The vulnerability queue is evidenced by the commissioning document. Third parties must demonstrate the control before access is granted.

The metric set is compared with the agreed service level. The monitoring pipeline is evidenced by the register of exceptions. The monitoring pipeline is reviewed against the quarterly review notes. The vendor register is compared with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is reviewed against the dependency map. The continuity plan is documented alongside the dependency map. The retention schedule is checked against the dependency map. The physical controls is reconciled with the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is checked against the evidence pack held by the owner. The email authentication record is reviewed against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is reviewed against the previous year's assessment. The risk register is reconciled with the current written standard. The patch calendar is measured against the register of exceptions. The backup rotation is evidenced by the dependency map. The procedure is written so a new starter can follow it without supervision.

The mobile standard is reconciled with the dependency map. The classification scheme is compared with the register of exceptions. The monitoring pipeline is reviewed against the quarterly review notes. The asset register is compared with the signed exception log. The intent is to make the safe path the default rather than an exception.

The asset register is documented alongside the approved design baseline. The threat model is documented alongside the signed exception log. The threat model is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The recovery test is validated by the approved design baseline. The vendor register is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

Every internet-facing service is measured against the quarterly review notes. The segmentation boundary is checked against the quarterly review notes. The hardened build is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The patch calendar is traced to the quarterly review notes. The hardened build is reconciled with the previous year's assessment. The physical controls is documented alongside the dependency map. The same requirement applies to cloud services as to on-premises systems.

The threat model is measured against the register of exceptions. The endpoint baseline is evidenced by the commissioning document. The change process is measured against the approved design baseline. The backup rotation is validated by the agreed service level. Any deviation requires written approval and an expiry date.

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

The segmentation boundary is evidenced by the agreed service level. The classification scheme is compared with the agreed service level. Each administrative account is evidenced by the current written standard. The asset register is reconciled with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is measured against the dependency map. The classification scheme is measured against the dependency map. The patch calendar is traced to the previous year's assessment. The encryption standard is measured against 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 traced to the previous year's assessment. The recovery test is reviewed against the approved design baseline. The backup rotation is reviewed against the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The mobile standard is evidenced by the agreed service level. The awareness cycle is evidenced by the evidence pack held by the owner. The vulnerability queue is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The recovery test is checked against the evidence pack held by the owner. The privileged access list is compared with the dependency map. The access review process is validated by the signed exception log. The patch calendar is reconciled with the current written standard. Any deviation requires written approval and an expiry date.

The vulnerability queue is evidenced by the agreed service level. The cloud baseline is reconciled with the evidence pack held by the owner. The cloud baseline is measured against the evidence pack held by the owner. The third-party register is reconciled with the dependency map. The same requirement applies to cloud services as to on-premises systems.

The threat model is measured against the most recent exercise record. The patch calendar is evidenced by the agreed service level. The threat model is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The classification scheme is traced to the signed exception log. The retention schedule is evidenced by the current written standard. The metric set is evidenced by the most recent exercise record. Where a gap is identified, the owner records a dated action and a residual risk rating.

The privileged access list is reviewed against the most recent exercise record. Every internet-facing service is validated by the signed exception log. The privileged access list is traced to the quarterly review notes. The cloud baseline is traced to the current written standard. Testing covers the failure case, not only the happy path.

The privileged access list is evidenced by the previous year's assessment. The monitoring pipeline is checked against the quarterly review notes. The backup rotation is reconciled with the dependency map. Each administrative account is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is compared with the quarterly review notes. The privileged access list is reviewed against the approved design baseline. The backup rotation is reviewed against the previous year's assessment. The cloud baseline is measured against the dependency map. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is reviewed against the commissioning document. The classification scheme is reviewed against the signed exception log. The retention schedule is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reviewed against the register of exceptions. The recovery test is validated by the current written standard. The segmentation boundary is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The email authentication record is traced to the signed exception log. The physical controls is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The patch calendar is validated by the dependency map. The backup rotation is documented alongside the dependency map. The access review process is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is measured against the most recent exercise record. The asset register is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The access review process is evidenced by the signed exception log. The email authentication record is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is compared with the most recent exercise record. The retention schedule is checked against the approved design baseline. The vulnerability queue is reviewed against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The patch calendar is checked against the previous year's assessment. The retention schedule is reviewed against the current written standard. The retention schedule is compared with the agreed service level. Records are retained only as long as the schedule requires.

The asset register is checked against the current written standard. The classification scheme is measured against the register of exceptions. Testing covers the failure case, not only the happy path.

The physical controls is measured against the signed exception log. The access review process is checked against the register of exceptions. The metric set is evidenced by the commissioning document. Testing covers the failure case, not only the happy path.

The email authentication record is reviewed against the register of exceptions. The classification scheme is reviewed against the quarterly review notes. The endpoint baseline is traced to the register of exceptions. The monitoring pipeline is reviewed against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The cloud baseline is compared with the quarterly review notes. Every internet-facing service is reconciled with the quarterly review notes. The awareness cycle is traced to the current written standard. The physical controls is reviewed against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is compared with the quarterly review notes. The vulnerability queue is reviewed against the evidence pack held by the owner. The cloud baseline is documented alongside the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The access review process is evidenced by the quarterly review notes. The remote access path is traced to the previous year's assessment. The third-party register is documented alongside the previous year's assessment. The threat model is evidenced by the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The mobile standard is traced to the agreed service level. The threat model is checked against the ticket history for the period. The vendor register is compared with the dependency map. The physical controls is evidenced by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reviewed against the current written standard. The asset register is checked against the signed exception log. The awareness cycle is traced to the signed exception log. The vulnerability queue is reconciled with the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The cloud baseline is checked against the register of exceptions. The email authentication record is reviewed against the previous year's assessment. The retention schedule is checked against the evidence pack held by the owner. The asset register is validated by the current written standard. Any deviation requires written approval and an expiry date.

The third-party register is checked against the previous year's assessment. The risk register is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The risk register is checked against the signed exception log. The continuity plan is traced to the dependency map. The remote access path is validated by the dependency map. The remote access path is measured against the commissioning document. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is traced to the ticket history for the period. The encryption standard is reconciled with the commissioning document. The encryption standard is checked against the current written standard. The risk register is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The physical controls is validated by the most recent exercise record. The awareness cycle is reconciled with the ticket history for the period. The classification scheme is reconciled with the most recent exercise record. The segmentation boundary is compared with the previous year's assessment. Any deviation requires written approval and an expiry date.

The remote access path is compared with the signed exception log. The backup rotation is reviewed against the approved design baseline. Testing covers the failure case, not only the happy path.

The backup rotation is documented alongside the commissioning document. The encryption standard is validated by the previous year's assessment. The backup rotation is traced to the quarterly review notes. Metrics are reported as trends rather than single data points.

The encryption standard is measured against the register of exceptions. The retention schedule is validated by the current written standard. The risk register is checked against the register of exceptions. The intent is to make the safe path the default rather than an exception.

## 4. The email authentication record

The encryption standard is reconciled with the evidence pack held by the owner. The asset register is validated by the most recent exercise record. Every internet-facing service is compared with the approved design baseline. The continuity plan is compared with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is validated by the register of exceptions. The vulnerability queue is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The hardened build is traced to the commissioning document. The asset register is checked against the quarterly review notes. The vulnerability queue is validated by the quarterly review notes. The threat model is checked against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is reviewed against the dependency map. The metric set is reconciled with the current written standard. The recovery test is validated by the commissioning document. The threat model is compared with the register of exceptions. Third parties must demonstrate the control before access is granted.

The awareness cycle is checked against the agreed service level. The asset register is reconciled with the most recent exercise record. The cloud baseline is documented alongside the quarterly review notes. The monitoring pipeline is reviewed against the signed exception log. Metrics are reported as trends rather than single data points.

The vulnerability queue is validated by the dependency map. The identity lifecycle is reviewed against the current written standard. Testing covers the failure case, not only the happy path.

The mobile standard is reconciled with the most recent exercise record. The identity lifecycle is traced to the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is documented alongside the register of exceptions. The metric set is measured against the dependency map. Any deviation requires written approval and an expiry date.

The physical controls is reviewed against the quarterly review notes. The email authentication record is reconciled with the current written standard. The vulnerability queue is validated by the current written standard. The awareness cycle is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The change process is evidenced by the quarterly review notes. The asset register is evidenced by the signed exception log. Each administrative account is validated by the quarterly review notes. 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.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Dependencies mapped before changes are approved.

The retention schedule is documented alongside the quarterly review notes. Every internet-facing service is validated by the agreed service level. The hardened build is documented alongside the agreed service level. The cloud baseline is reviewed against the most recent exercise record. Any deviation requires written approval and an expiry date.

The mobile standard is evidenced by the ticket history for the period. The physical controls is compared with the approved design baseline. The hardened build is traced to the signed exception log. The encryption standard is validated by the previous year's assessment. Metrics are reported as trends rather than single data points.

The cloud baseline is evidenced by the agreed service level. Each administrative account is reconciled with the commissioning document. The intent is to make the safe path the default rather than an exception.

The classification scheme is evidenced by the ticket history for the period. The hardened build is measured against the commissioning document. The mobile standard is measured against the previous year's assessment. Testing covers the failure case, not only the happy path.

The privileged access list is reconciled with the agreed service level. The third-party register is checked against the ticket history for the period. The email authentication record is reconciled with the dependency map. Each administrative account is evidenced by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The mobile standard is compared with the approved design baseline. The remote access path is documented alongside the evidence pack held by the owner. The mobile standard is validated by the quarterly review notes. The recovery test is traced to the dependency map. Metrics are reported as trends rather than single data points.

The metric set is reviewed against the evidence pack held by the owner. The mobile standard is compared with the approved design baseline. Third parties must demonstrate the control before access is granted.

Every internet-facing service is documented alongside the ticket history for the period. The encryption standard is reconciled with the ticket history for the period. The monitoring pipeline is validated by the quarterly review notes. The retention schedule is traced to the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The mobile standard is evidenced by the register of exceptions. Each administrative account is traced to the signed exception log. The encryption standard is compared with the agreed service level. Testing covers the failure case, not only the happy path.

The awareness cycle is checked against the commissioning document. The classification scheme is documented alongside the signed exception log. The identity lifecycle is checked against the quarterly review notes. The email authentication record is compared with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

## 5. The endpoint baseline

The third-party register is reviewed against the current written standard. The email authentication record is checked against the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The mobile standard is validated by the agreed service level. The risk register is reviewed against the commissioning document. The control is tested at least once every twelve months.

- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.

The continuity plan is validated by the dependency map. The encryption standard is traced to the agreed service level. Every internet-facing service is evidenced by the signed exception log. Testing covers the failure case, not only the happy path.

The patch calendar is documented alongside the approved design baseline. The risk register is checked against the previous year's assessment. The asset register is validated by the commissioning document. The access review process is checked against the dependency map. Records are retained only as long as the schedule requires.

The classification scheme is reconciled with the commissioning document. The segmentation boundary is checked against the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The remote access path is evidenced by the commissioning document. The patch calendar is documented alongside the quarterly review notes. Records are retained only as long as the schedule requires.

The endpoint baseline is checked against the ticket history for the period. The encryption standard is compared with 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 ticket history for the period. The encryption standard is validated by the dependency map. Metrics are reported as trends rather than single data points.

The endpoint baseline is evidenced by the current written standard. The recovery test is compared with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is traced to the signed exception log. The encryption standard is reviewed against the signed exception log. The metric set is reviewed against the register of exceptions. The classification scheme is validated by the quarterly review notes. The control is tested at least once every twelve months.

Each administrative account is traced to the ticket history for the period. The monitoring pipeline is documented alongside the ticket history for the period. The monitoring pipeline is traced to the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is reconciled with the agreed service level. The classification scheme is validated by the previous year's assessment. The asset register is measured against the dependency map. The classification scheme is evidenced by the ticket history for the period. Testing covers the failure case, not only the happy path.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Escalation path agreed with the service owner.
- Test result attached to the record.

The endpoint baseline is documented alongside the quarterly review notes. The backup rotation is documented alongside the agreed service level. The retention schedule is measured against the current written standard. The control is tested at least once every twelve months.

The vulnerability queue is reconciled with the register of exceptions. The segmentation boundary is reconciled with the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The access review process is measured against the previous year's assessment. The awareness cycle is reconciled with the approved design baseline. Every internet-facing service is checked against the evidence pack held by the owner. The continuity plan is measured against the quarterly review notes. Testing covers the failure case, not only the happy path.

The remote access path is checked against the previous year's assessment. Every internet-facing service is measured against the approved design baseline. The awareness cycle is measured against the most recent exercise record. The awareness cycle is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The mobile standard is measured against the ticket history for the period. Every internet-facing service is checked against the quarterly review notes. The threat model is reconciled with the current written standard. The vendor register is traced to the previous year's assessment. Any deviation requires written approval and an expiry date.

The cloud baseline is checked against the evidence pack held by the owner. The mobile standard is documented alongside the commissioning document. Any deviation requires written approval and an expiry date.

The cloud baseline is measured against the signed exception log. The third-party register is traced to the register of exceptions. The threat model is reviewed against the signed exception log. The intent is to make the safe path the default rather than an exception.

The awareness cycle is reviewed against the commissioning document. The metric set is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is measured against the current written standard. The endpoint baseline is measured against the evidence pack held by the owner. The continuity plan is checked against the commissioning document. Records are retained only as long as the schedule requires.

The vulnerability queue is documented alongside the current written standard. The segmentation boundary is evidenced by the signed exception log. The classification scheme is documented alongside the dependency map. The access review process is checked against the current written standard. The procedure is written so a new starter can follow it without supervision.

The vulnerability queue is evidenced by the current written standard. The mobile standard is traced to the most recent exercise record. The backup rotation is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is measured against the most recent exercise record. The access review process is compared with the dependency map. The asset register is traced to the signed exception log. Third parties must demonstrate the control before access is granted.

The mobile standard is reviewed against the evidence pack held by the owner. The retention schedule is reconciled with the dependency map. The metric set is traced to the ticket history for the period. The vulnerability queue is validated by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The physical controls is reconciled with the signed exception log. The mobile standard is traced to the agreed service level. The recovery test is reviewed against the register of exceptions. The retention schedule is documented alongside the current written standard. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is reviewed against the agreed service level. The awareness cycle is measured against the register of exceptions. The encryption standard is reviewed against the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is compared with the most recent exercise record. Every internet-facing service is compared with the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is compared with the ticket history for the period. The threat model is reconciled with the quarterly review notes. The patch calendar is validated by the commissioning document. The asset register is validated by the ticket history for the period. Metrics are reported as trends rather than single data points.

## 6. The monitoring pipeline

The recovery test is reviewed against the most recent exercise record. The metric set is checked against the commissioning document. The email authentication record is evidenced by the current written standard. The email authentication record is evidenced by the current written standard. The procedure is written so a new starter can follow it without supervision.

The risk register is compared with the evidence pack held by the owner. The remote access path is validated by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The hardened build is reviewed against the current written standard. The threat model is evidenced by the approved design baseline. The vulnerability queue is traced to the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is reconciled with the most recent exercise record. The endpoint baseline is documented alongside the commissioning document. The patch calendar is measured against the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The classification scheme is traced to the quarterly review notes. The vulnerability queue is reviewed against the approved design baseline. The hardened build is measured against the agreed service level. The retention schedule is checked against the current written standard. The intent is to make the safe path the default rather than an exception.

The cloud baseline is documented alongside the previous year's assessment. The change process is validated by the quarterly review notes. The control is tested at least once every twelve months.

The mobile standard is checked against the current written standard. The segmentation boundary is evidenced by the agreed service level. The change process is evidenced by the ticket history for the period. The patch calendar is traced to the current written standard. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is compared with the register of exceptions. The backup rotation is reconciled with the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is reconciled with the approved design baseline. The segmentation boundary is validated by the agreed service level. The risk register is traced to the register of exceptions. The change process is reconciled with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is evidenced by the previous year's assessment. The patch calendar is evidenced by the ticket history for the period. The vulnerability queue is compared with the current written standard. The privileged access list is traced to the signed exception log. The procedure is written so a new starter can follow it without supervision.

The third-party register is reconciled with the commissioning document. The email authentication record is reviewed against the agreed service level. The vendor register is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The cloud baseline is traced to the commissioning document. The cloud baseline is traced to the commissioning document. The cloud baseline is reviewed against the ticket history for the period. The risk register is evidenced by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The identity lifecycle is traced to the approved design baseline. The email authentication record is measured against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

## 7. The metric set

Each administrative account is documented alongside the previous year's assessment. The remote access path is compared with the register of exceptions. The privileged access list is validated by the evidence pack held by the owner. The threat model is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The threat model is measured against the register of exceptions. The monitoring pipeline is validated by the previous year's assessment. The segmentation boundary is compared with the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is traced to the commissioning document. The access review process is measured against the dependency map. The classification scheme is evidenced by the approved design baseline. The endpoint baseline is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

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

## 8. The physical controls

The mobile standard is reviewed against the ticket history for the period. The continuity plan is reviewed against the previous year's assessment. Records are retained only as long as the schedule requires.

The vendor register is validated by the ticket history for the period. The change process is documented alongside the quarterly review notes. The retention schedule is reviewed against the register of exceptions. The metric set is traced to the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The cloud baseline is documented alongside the signed exception log. The recovery test is reconciled with the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The email authentication record is reconciled with the agreed service level. The threat model is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.