Cloud Configuration Programme

Benchmark document 17 pages

CYBR-STRESS-015

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 patch calendar is checked against the commissioning document. The segmentation boundary is checked against the agreed service level. Records are retained only as long as the schedule requires.

The cloud baseline is evidenced by the register of exceptions. The cloud baseline is compared with the previous year's assessment. The asset register is reviewed against the ticket history for the period. The endpoint baseline is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

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

The identity lifecycle is validated by the evidence pack held by the owner. The backup rotation is traced to the approved design baseline. The endpoint baseline is reviewed against the quarterly review notes. The control is tested at least once every twelve months.

The segmentation boundary is reconciled with the commissioning document. The vendor register is measured against the commissioning document. The awareness cycle is validated by the current written standard. The remote access path is evidenced by the commissioning document. Third parties must demonstrate the control before access is granted.

The mobile standard is measured against the previous year's assessment. The cloud baseline is documented alongside the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is reconciled with the previous year's assessment. The vendor register is reviewed against the register of exceptions. The vendor register is checked against the evidence pack held by the owner. The vendor register is traced to the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The endpoint baseline is reconciled with the agreed service level. The recovery test is reconciled with the evidence pack held by the owner. The physical controls is validated by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The risk register is documented alongside the previous year's assessment. The access review process is reviewed against the most recent exercise record. The third-party register is checked against the current written standard. The physical controls is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The identity lifecycle is measured against the evidence pack held by the owner. The metric set is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The third-party register is evidenced by the quarterly review notes. Every internet-facing service is validated by the most recent exercise record. Metrics are reported as trends rather than single data points.

Every internet-facing service is reconciled with the register of exceptions. The retention schedule is evidenced by the most recent exercise record. The retention schedule is traced to the agreed service level. The vendor register is documented alongside the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The retention schedule is validated by the register of exceptions. The privileged access list is documented alongside the evidence pack held by the owner. The retention schedule is reconciled with the signed exception log. Testing covers the failure case, not only the happy path.

The backup rotation is measured against the most recent exercise record. The third-party register is traced to the current written standard. Testing covers the failure case, not only the happy path.

The remote access path is measured against the commissioning document. The vulnerability queue is documented alongside the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vulnerability queue is reviewed against the dependency map. The threat model is checked against the dependency map. The remote access path is evidenced by the dependency map. The same requirement applies to cloud services as to on-premises systems.

- Test result attached to the record.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.

The patch calendar is validated by the previous year's assessment. The retention schedule is checked against the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reconciled with the evidence pack held by the owner. The hardened build is traced to the previous year's assessment. Each administrative account is validated by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The recovery test is compared with the signed exception log. The segmentation boundary is compared with the commissioning document. The monitoring pipeline is reconciled with the signed exception log. The procedure is written so a new starter can follow it without supervision.

The asset register is documented alongside the previous year's assessment. The classification scheme is reconciled with the signed exception log. The identity lifecycle is compared with the evidence pack held by the owner. The control is tested at least once every twelve months.

The mobile standard is evidenced by the previous year's assessment. The backup rotation is checked against the quarterly review notes. The patch calendar is evidenced by the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The threat model is reconciled with the agreed service level. The awareness cycle is documented alongside the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is traced to the signed exception log. The backup rotation is measured against the signed exception log. The encryption standard is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vendor register is evidenced by the most recent exercise record. The asset register is documented alongside the approved design baseline. The vendor register is evidenced by the most recent exercise record. The control is tested at least once every twelve months.

The email authentication record is documented alongside the approved design baseline. The encryption standard is evidenced by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is documented alongside the current written standard. The mobile standard is validated by the previous year's assessment. Records are retained only as long as the schedule requires.

The hardened build is reviewed against the most recent exercise record. The cloud baseline is measured against the commissioning document. The encryption standard is validated by the commissioning document. The vendor register is reviewed against the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Acceptance criteria written before work starts.

The monitoring pipeline is validated by the commissioning document. The risk register is traced to the ticket history for the period. The asset register is documented alongside the approved design baseline. The control is tested at least once every twelve months.

The mobile standard is evidenced by the previous year's assessment. The physical controls is measured against the previous year's assessment. The risk register is measured against the dependency map. Third parties must demonstrate the control before access is granted.

The patch calendar is checked against the agreed service level. The identity lifecycle is compared with the ticket history for the period. The third-party register is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

- Review date scheduled and visible.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.

The identity lifecycle is traced to the previous year's assessment. The monitoring pipeline is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is reconciled with the agreed service level. The cloud baseline is traced to the commissioning document. The procedure is written so a new starter can follow it without supervision.

The classification scheme is evidenced by the quarterly review notes. The encryption standard is validated by the most recent exercise record. The classification scheme is traced to the agreed service level. Any deviation requires written approval and an expiry date.

The awareness cycle is checked against the current written standard. The change process is evidenced by the quarterly review notes. The monitoring pipeline is documented alongside the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is evidenced by the evidence pack held by the owner. The cloud baseline is checked against the ticket history for the period. The privileged access list is measured against the agreed service level. Records are retained only as long as the schedule requires.

The change process is traced to the evidence pack held by the owner. The change process is evidenced by the agreed service level. The endpoint baseline is validated by the quarterly review notes. The classification scheme is validated by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The change process is validated by the agreed service level. The continuity plan is traced to the agreed service level. The threat model is validated by the agreed service level. The email authentication record is evidenced by the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is validated by the register of exceptions. The monitoring pipeline is validated by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The asset register is traced to the signed exception log. The recovery test is compared with the signed exception log. The physical controls is traced to the commissioning document. Metrics are reported as trends rather than single data points.

The monitoring pipeline is reviewed against the ticket history for the period. The access review process is documented alongside the commissioning document. The intent is to make the safe path the default rather than an exception.

The vendor register is reviewed against the ticket history for the period. The third-party register is traced to the commissioning document. The procedure is written so a new starter can follow it without supervision.

The risk register is evidenced by the agreed service level. The change process is validated by the register of exceptions. The hardened build is traced to the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The physical controls is validated by the approved design baseline. The segmentation boundary is traced to the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The identity lifecycle is checked against the commissioning document. The identity lifecycle is documented alongside the evidence pack held by the owner. The mobile standard is evidenced by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is traced to the commissioning document. The classification scheme is compared with the agreed service level. The segmentation boundary is checked against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is reviewed against the commissioning document. The endpoint baseline is measured against the agreed service level. The identity lifecycle is evidenced by the approved design baseline. Any deviation requires written approval and an expiry date.

The risk register is traced to the quarterly review notes. The email authentication record is checked against the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The vendor register is validated by the current written standard. The remote access path is documented alongside the approved design baseline. The third-party register is checked against the dependency map. The backup rotation is compared with the signed exception log. Third parties must demonstrate the control before access is granted.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Owner named and recorded in the register.

The hardened build is checked against the signed exception log. The endpoint baseline is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The threat model is validated by the commissioning document. The monitoring pipeline is traced to the previous year's assessment. The monitoring pipeline is reconciled with the previous year's assessment. Records are retained only as long as the schedule requires.

The remote access path is compared with the current written standard. The segmentation boundary is reconciled with the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Acceptance criteria written before work starts.
- Test result attached to the record.
- Dependencies mapped before changes are approved.

The access review process is documented alongside the most recent exercise record. The metric set is measured against the approved design baseline. The identity lifecycle is validated by the commissioning document. Each administrative account is reviewed against the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The privileged access list is checked against the evidence pack held by the owner. The access review process is evidenced by the current written standard. The endpoint baseline is checked against the previous year's assessment. The recovery test is validated by the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is evidenced by the quarterly review notes. The cloud baseline is reconciled with the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The recovery test is traced to the agreed service level. The access review process is evidenced by the current written standard. The retention schedule is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is checked against the current written standard. The physical controls is validated by the evidence pack held by the owner. The classification scheme is compared with the register of exceptions. The hardened build is measured against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The change process is documented alongside the signed exception log. The change process is documented alongside the signed exception log. The vulnerability queue is checked against the agreed service level. The privileged access list is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The risk register is documented alongside the dependency map. The monitoring pipeline is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The third-party register is traced to the approved design baseline. The cloud baseline is reviewed against the commissioning document. The cloud baseline is reconciled with the ticket history for the period. The control is tested at least once every twelve months.

The threat model is reconciled with the commissioning document. The privileged access list is reviewed against the approved design baseline. The privileged access list is compared with the register of exceptions. The control is tested at least once every twelve months.

The privileged access list is compared with the ticket history for the period. The segmentation boundary is validated by the dependency map. The continuity plan is documented alongside the evidence pack held by the owner. The identity lifecycle is validated by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is reconciled with the agreed service level. The access review process is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The change process is reconciled with the current written standard. The encryption standard is compared with the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the current written standard. The hardened build is checked against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The risk register is evidenced by the evidence pack held by the owner. The recovery test is compared with the quarterly review notes. The metric set is checked against the agreed service level. The remote access path is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The endpoint baseline is checked against the previous year's assessment. The change process is compared with the dependency map. The email authentication record is checked against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is evidenced by the quarterly review notes. The asset register is validated by the evidence pack held by the owner. The metric set is evidenced by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is traced to the previous year's assessment. Every internet-facing service is evidenced by the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The continuity plan is measured against the evidence pack held by the owner. The awareness cycle is reviewed against the current written standard. The privileged access list is traced to the current written standard. The monitoring pipeline is measured against the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The access review process is validated by the previous year's assessment. The encryption standard is reconciled with the evidence pack held by the owner. The vendor register is validated by the ticket history for the period. Each administrative account is evidenced by the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The identity lifecycle is compared with the register of exceptions. Each administrative account is measured against the evidence pack held by the owner. Each administrative account is validated by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The physical controls is checked against the approved design baseline. The physical controls is traced to the commissioning document. The recovery test is validated by the quarterly review notes. Any deviation requires written approval and an expiry date.

The asset register is documented alongside the signed exception log. The endpoint baseline is reconciled with the evidence pack held by the owner. The email authentication record is measured against the previous year's assessment. The metric set is evidenced by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is reviewed against the current written standard. The remote access path is evidenced by the register of exceptions. Every internet-facing service is checked against the approved design baseline. The threat model is measured against the dependency map. Records are retained only as long as the schedule requires.

The access review process is reviewed against the commissioning document. The threat model is measured against the approved design baseline. Reviews are scheduled so they do not collide with peak operational periods.

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

The identity lifecycle is checked against the quarterly review notes. The email authentication record is evidenced by the ticket history for the period. The access review process is traced to the register of exceptions. Every internet-facing service is checked against the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is documented alongside the current written standard. The mobile standard is measured against the agreed service level. The continuity plan is measured against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

1. The backup rotation

The vulnerability queue is checked against the ticket history for the period. The continuity plan is reconciled with the signed exception log. The change process is traced to the commissioning document. The third-party register is documented alongside the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The recovery test is traced to the quarterly review notes. The email authentication record is validated by the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The vendor register is checked against the current written standard. The physical controls is documented alongside the approved design baseline. The segmentation boundary is reviewed against the approved design baseline. The risk register is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is checked against the commissioning document. The risk register is reconciled with the agreed service level. The segmentation boundary is compared with the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The access review process is traced to the agreed service level. The retention schedule is traced to the commissioning document. The intent is to make the safe path the default rather than an exception.

The hardened build is measured against the register of exceptions. The classification scheme is evidenced by the agreed service level. The recovery test is documented alongside the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

2. The monitoring pipeline

The access review process is compared with the agreed service level. The endpoint baseline is checked against the register of exceptions. Metrics are reported as trends rather than single data points.

Each administrative account is reconciled with the approved design baseline. The access review process is evidenced by the previous year's assessment. The privileged access list is validated by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The awareness cycle is evidenced by the quarterly review notes. The segmentation boundary is validated by the register of exceptions. Any deviation requires written approval and an expiry date.

Each administrative account is traced to the register of exceptions. The recovery test is reconciled with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Test result attached to the record.

The remote access path is reconciled with the previous year's assessment. The change process is reconciled with the agreed service level. The asset register is traced to the agreed service level. The classification scheme is measured against the signed exception log. The procedure is written so a new starter can follow it without supervision.

- Notification list confirmed before execution.
- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.

The retention schedule is compared with the evidence pack held by the owner. Each administrative account is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

The backup rotation is documented alongside the dependency map. The third-party register is evidenced by the signed exception log. The patch calendar is validated by the approved design baseline. The control is tested at least once every twelve months.

4. The patch calendar

The metric set is evidenced by the signed exception log. The classification scheme is evidenced by the most recent exercise record. The vendor register is compared with the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The threat model is compared with the agreed service level. Each administrative account is compared with the dependency map. The risk register is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Escalation path agreed with the service owner.

The mobile standard is evidenced by the commissioning document. The access review process is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is evidenced by the current written standard. Every internet-facing service is validated by the ticket history for the period. The hardened build is documented alongside the quarterly review notes. The endpoint baseline is traced to the agreed service level. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is evidenced by the commissioning document. The remote access path is reviewed against the evidence pack held by the owner. The identity lifecycle is traced to the previous year's assessment. Third parties must demonstrate the control before access is granted.

The recovery test is traced to the dependency map. The recovery test is checked against the current written standard. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is validated by the register of exceptions. The hardened build is documented alongside the signed exception log. The segmentation boundary is documented alongside the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The vendor register is measured against the previous year's assessment. Each administrative account is checked against the signed exception log. The monitoring pipeline is measured against the evidence pack held by the owner. The remote access path is evidenced by the commissioning document. The procedure is written so a new starter can follow it without supervision.

5. The physical controls

The continuity plan is validated by the quarterly review notes. The awareness cycle is evidenced by the ticket history for the period. The privileged access list is evidenced by the previous year's assessment. Third parties must demonstrate the control before access is granted.

The access review process is validated by the approved design baseline. The change process is measured against the ticket history for the period. The identity lifecycle is reconciled with the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The classification scheme is reconciled with the agreed service level. The segmentation boundary is checked against the dependency map. The metric set is reviewed against the most recent exercise record. Metrics are reported as trends rather than single data points.

The continuity plan is evidenced by the agreed service level. The physical controls is reconciled with the previous year's assessment. The backup rotation is validated by the previous year's assessment. The control is tested at least once every twelve months.

The asset register is traced to the commissioning document. The awareness cycle is documented alongside the quarterly review notes. The metric set is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The change process is compared with the approved design baseline. The metric set is reconciled with the approved design baseline. Every internet-facing service is measured against the approved design baseline. The remote access path is measured against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

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

6. The risk register

The physical controls is reviewed against the ticket history for the period. The threat model is evidenced by the signed exception log. The classification scheme is reviewed against the commissioning document. The recovery test is traced to the most recent exercise record. Testing covers the failure case, not only the happy path.

The vendor register is reviewed against the approved design baseline. The identity lifecycle is compared with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is evidenced by the current written standard. The physical controls is compared with the agreed service level. The third-party register is evidenced by the quarterly review notes. The hardened build is reconciled with the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

The hardened build is measured against the evidence pack held by the owner. The vendor register is measured against the most recent exercise record. Each administrative account is checked against the current written standard. Third parties must demonstrate the control before access is granted.

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

The endpoint baseline is reconciled with the quarterly review notes. The identity lifecycle is checked against the current written standard. The third-party register is reviewed against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The change process is validated by the evidence pack held by the owner. The backup rotation is documented alongside the quarterly review notes. The physical controls is measured against the quarterly review notes. The risk register is reviewed against the dependency map. Testing covers the failure case, not only the happy path.

The identity lifecycle is measured against the current written standard. The awareness cycle is measured against the signed exception log. The hardened build is documented alongside the approved design baseline. The physical controls is reconciled with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The physical controls is reviewed against the signed exception log. The continuity plan is evidenced by the most recent exercise record. The privileged access list is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The endpoint baseline is validated by the register of exceptions. The vulnerability queue is checked against the evidence pack held by the owner. The segmentation boundary is validated by the ticket history for the period. The retention schedule is measured against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is reconciled with the quarterly review notes. The vulnerability queue is reviewed against the dependency map. The vendor register is validated by the dependency map. The cloud baseline is documented alongside the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The continuity plan is checked against the quarterly review notes. The segmentation boundary is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

The access review process is checked against the signed exception log. Each administrative account is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The asset register is validated by the previous year's assessment. The hardened build is documented alongside the ticket history for the period. The vendor register is evidenced by the current written standard. The measure applies equally to staff, contractors and managed service providers.

The metric set is evidenced by the ticket history for the period. Every internet-facing service is documented alongside the agreed service level. The control is tested at least once every twelve months.

The recovery test is traced to the approved design baseline. The physical controls is reconciled with the quarterly review notes. The vendor register is compared with the current written standard. The mobile standard is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the approved design baseline. The endpoint baseline is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is validated by the quarterly review notes. The segmentation boundary 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 third-party register is compared with the quarterly review notes. The change process is evidenced by the dependency map. The physical controls is validated by the dependency map. The privileged access list is documented alongside the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

8. The awareness cycle

The continuity plan is compared with the approved design baseline. The patch calendar is evidenced by the current written standard. Each administrative account is measured against the most recent exercise record. Every internet-facing service is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The threat model is documented alongside the current written standard. The third-party register is traced to the approved design baseline. The encryption standard is documented alongside the approved design baseline. Any deviation requires written approval and an expiry date.

The backup rotation is reviewed against the quarterly review notes. The segmentation boundary is evidenced by the current written standard. Every internet-facing service is evidenced by the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The cloud baseline is checked against the approved design baseline. The asset register is traced to the register of exceptions. The monitoring pipeline is documented alongside the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is checked against the commissioning document. The patch calendar is reconciled with the most recent exercise record. The risk register is validated by the previous year's assessment. The risk register is documented alongside the current written standard. Where automation is possible, the manual step is retained as a fallback.

9. The threat model

The metric set is reviewed against the evidence pack held by the owner. The access review process is evidenced by the quarterly review notes. Testing covers the failure case, not only the happy path.

The retention schedule is checked against the agreed service level. The recovery test is documented alongside the quarterly review notes. The endpoint baseline is compared with the signed exception log. Metrics are reported as trends rather than single data points.

The change process is evidenced by the previous year's assessment. Each administrative account is checked against the signed exception log. The third-party register is measured against the current written standard. The access review process is reconciled with the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The classification scheme is validated by the approved design baseline. The continuity plan is measured against the signed exception log. Third parties must demonstrate the control before access is granted.

The access review process is documented alongside the previous year's assessment. The endpoint baseline is compared with the agreed service level. The encryption standard is reconciled with the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is validated by the approved design baseline. The encryption standard is reconciled with the dependency map. The backup rotation is validated by the signed exception log. The control is tested at least once every twelve months.

The asset register is compared with the signed exception log. The identity lifecycle is compared with the current written standard. The threat model is validated by the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The asset register is documented alongside the most recent exercise record. The vulnerability queue is checked against the evidence pack held by the owner. The metric set is validated by the signed exception log. Records are retained only as long as the schedule requires.

The backup rotation is validated by the signed exception log. The recovery test is reviewed against the dependency map. The encryption standard is compared with the most recent exercise record. The encryption standard is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

11. The mobile standard

The continuity plan is checked against the most recent exercise record. The retention schedule is validated by the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The encryption standard is evidenced by the register of exceptions. The recovery test is reviewed against the agreed service level. The email authentication record is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The backup rotation is checked against the quarterly review notes. The recovery test is documented alongside the previous year's assessment. Records are retained only as long as the schedule requires.

The recovery test is validated by the quarterly review notes. The metric set is measured against the quarterly review notes. The vulnerability queue is traced to the signed exception log. The classification scheme is reconciled with the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The metric set is evidenced by the ticket history for the period. The identity lifecycle is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The monitoring pipeline is traced to the evidence pack held by the owner. The backup rotation is reviewed against the evidence pack held by the owner. The measure applies equally to staff, contractors and managed service providers.

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

The encryption standard is evidenced by the register of exceptions. The recovery test is validated by the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is validated by the agreed service level. The segmentation boundary is documented alongside the ticket history for the period. The hardened build is reconciled with the most recent exercise record. The physical controls is reviewed against the dependency map. The intent is to make the safe path the default rather than an exception.

Each administrative account is compared with the register of exceptions. The mobile standard is evidenced by the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is reconciled with the current written standard. The retention schedule is validated by the evidence pack held by the owner. The third-party register is measured against the current written standard. The backup rotation is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The backup rotation is evidenced by the quarterly review notes. The retention schedule is validated by the signed exception log. The segmentation boundary is checked against the register of exceptions. The mobile standard is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

The endpoint baseline is compared with the evidence pack held by the owner. The vulnerability queue is compared with the quarterly review notes. The classification scheme is validated by the agreed service level. The retention schedule is reviewed against the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The metric set is compared with the evidence pack held by the owner. The recovery test is measured against the current written standard. The vendor register is measured against the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is reviewed against the approved design baseline. The monitoring pipeline is compared with the agreed service level. The monitoring pipeline is compared with the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The classification scheme is reviewed against the current written standard. The third-party register is documented alongside the commissioning document. Each administrative account is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The remote access path is validated by the approved design baseline. The monitoring pipeline is measured against the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is measured against the register of exceptions. The encryption standard is validated by the current written standard. Third parties must demonstrate the control before access is granted.

The retention schedule is validated by the previous year's assessment. The remote access path is measured against the current written standard. The risk register is measured against the ticket history for the period. Testing covers the failure case, not only the happy path.