Vendor Risk Standard

Exercise record 23 pages

CYBR-STRESS-009

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 compared with the approved design baseline. The email authentication record is documented alongside the most recent exercise record. The identity lifecycle is evidenced by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is compared with the agreed service level. The hardened build is checked against the previous year's assessment. The email authentication record is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The threat model is measured against the evidence pack held by the owner. The metric set is evidenced by the approved design baseline. The retention schedule is documented alongside the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is measured against the quarterly review notes. The third-party register is compared with the previous year's assessment. The endpoint baseline is reviewed 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 evidenced by the ticket history for the period. The segmentation boundary is reviewed against the dependency map. The intent is to make the safe path the default rather than an exception.

The classification scheme is documented alongside the dependency map. The continuity plan is validated by the approved design baseline. Every internet-facing service is compared with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is validated by the evidence pack held by the owner. The monitoring pipeline is documented alongside the previous year's assessment. The remote access path is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The continuity plan is compared with the quarterly review notes. The third-party register is reconciled with the agreed service level. The awareness cycle is documented alongside the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The segmentation boundary is documented alongside the register of exceptions. The classification scheme is measured against the register of exceptions. The threat model is reconciled with the current written standard. The encryption standard is measured against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is validated by the dependency map. The identity lifecycle is compared with the current written standard. The mobile standard is validated by the commissioning document. The endpoint baseline is compared with the commissioning document. The control is tested at least once every twelve months.

The recovery test is validated by the current written standard. The access review process is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The backup rotation is measured against the quarterly review notes. The risk register is traced to the most recent exercise record. The metric set is checked against the most recent exercise record. The cloud baseline is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The asset register is checked against the most recent exercise record. The awareness cycle is evidenced by the ticket history for the period. Third parties must demonstrate the control before access is granted.

1. The identity lifecycle

The classification scheme is measured against the agreed service level. The hardened build is traced to the evidence pack held by the owner. The retention schedule is reviewed against the current written standard. Records are retained only as long as the schedule requires.

The classification scheme is validated by the ticket history for the period. The encryption standard is reconciled with the ticket history for the period. Metrics are reported as trends rather than single data points.

- Notification list confirmed before execution.
- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.

The privileged access list is validated by the previous year's assessment. The threat model is evidenced by the most recent exercise record. The control is tested at least once every twelve months.

The continuity plan is compared with the quarterly review notes. The change process is traced to the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The change process is checked against the signed exception log. The change process is validated by the register of exceptions. The continuity plan is traced to the current written standard. The metric set is validated by the commissioning document. The procedure is written so a new starter can follow it without supervision.

The recovery test is traced to the dependency map. The threat model is compared with the signed exception log. The continuity plan is reconciled with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The recovery test is measured against the approved design baseline. The risk register is traced to the current written standard. The third-party register is validated by the previous year's assessment. The awareness cycle is checked against the most recent exercise record. Metrics are reported as trends rather than single data points.

The access review process is checked against the approved design baseline. The physical controls is reconciled with the register of exceptions. Records are retained only as long as the schedule requires.

The backup rotation is traced to the previous year's assessment. The threat model is evidenced by the quarterly review notes. The change process is traced to the approved design baseline. The vendor register is measured against the quarterly review notes. Metrics are reported as trends rather than single data points.

The asset register is traced to the current written standard. The recovery test is documented alongside the quarterly review notes. Each administrative account is checked against the approved design baseline. The backup rotation is compared with the agreed service level. Metrics are reported as trends rather than single data points.

The hardened build is validated by the dependency map. The threat model is compared with the current written standard. The monitoring pipeline is validated by the signed exception log. The threat model is checked against the previous year's assessment. Testing covers the failure case, not only the happy path.

The threat model is validated by the signed exception log. The encryption standard is measured against the ticket history for the period. The awareness cycle is validated by the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is reviewed against the previous year's assessment. The hardened build is compared with the quarterly review notes. The recovery test is documented alongside the quarterly review notes. The monitoring pipeline is checked against the current written standard. The control is tested at least once every twelve months.

The cloud baseline is compared with the dependency map. The mobile standard is reviewed against the most recent exercise record. Records are retained only as long as the schedule requires.

The vendor register is traced to the agreed service level. The risk register is reconciled with the most recent exercise record. Metrics are reported as trends rather than single data points.

The vulnerability queue is measured against the commissioning document. The risk register is compared with the evidence pack held by the owner. The recovery test is documented alongside the current written standard. Records are retained only as long as the schedule requires.

The identity lifecycle is evidenced by the signed exception log. The vendor register is reviewed against the most recent exercise record. The patch calendar is validated by the most recent exercise record. The hardened build is traced to the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The physical controls is documented alongside the dependency map. The privileged access list is checked against the register of exceptions. The hardened build is traced to the previous year's assessment. Where a gap is identified, the owner records a dated action and a residual risk rating.

The patch calendar is measured against the approved design baseline. The encryption standard is traced to the dependency map. The segmentation boundary is compared with the current written standard. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is traced to the register of exceptions. The identity lifecycle is compared with the current written standard. The encryption standard is measured against the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The physical controls is traced to the previous year's assessment. The threat model is compared with the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The recovery test is compared with the commissioning document. The retention schedule is documented alongside the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.
- Test result attached to the record.

The segmentation boundary is measured against the most recent exercise record. The vulnerability queue is checked against the most recent exercise record. The backup rotation is traced to the evidence pack held by the owner. The patch calendar is traced to the agreed service level. Metrics are reported as trends rather than single data points.

The asset register is evidenced by the ticket history for the period. The backup rotation is compared with the agreed service level. Any deviation requires written approval and an expiry date.

The access review process is traced to the commissioning document. The continuity plan is traced to the most recent exercise record. The retention schedule is reviewed against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The retention schedule is checked against the current written standard. Each administrative account is evidenced by the agreed service level. The third-party register is traced to the agreed service level. Third parties must demonstrate the control before access is granted.

The access review process is traced to the signed exception log. The email authentication record is validated by the ticket history for the period. Records are retained only as long as the schedule requires.

The backup rotation is checked against the register of exceptions. The vendor register is traced to the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The physical controls is evidenced by the signed exception log. The awareness cycle is checked against the current written standard. Metrics are reported as trends rather than single data points.

The vendor register is traced to the commissioning document. The monitoring pipeline is compared with the commissioning document. The third-party register is checked against the agreed service level. The intent is to make the safe path the default rather than an exception.

- Owner named and recorded in the register.
- Dependencies mapped before changes are approved.
- Test result attached to the record.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.

The awareness cycle is compared with the ticket history for the period. Every internet-facing service is checked against the agreed service level. The awareness cycle is compared with the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

Every internet-facing service is traced to the most recent exercise record. The patch calendar is compared with the ticket history for the period. Every internet-facing service is checked against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The encryption standard is evidenced by the previous year's assessment. The threat model is measured against the commissioning document. The monitoring pipeline is validated by the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is evidenced by the signed exception log. The encryption standard is checked against the current written standard. The awareness cycle is measured against the commissioning document. The email authentication record is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The risk register is traced to the dependency map. The vulnerability queue is compared with the register of exceptions. The continuity plan is validated by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reviewed against the register of exceptions. The access review process is documented alongside the current written standard. Testing covers the failure case, not only the happy path.

The access review process is evidenced by the current written standard. The hardened build is measured against the evidence pack held by the owner. The risk register is measured against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The cloud baseline is traced to the current written standard. The identity lifecycle is compared with the commissioning document. The encryption standard is validated by the quarterly review notes. The recovery test is reconciled with the approved design baseline. Any deviation requires written approval and an expiry date.

The identity lifecycle is compared with the previous year's assessment. The continuity plan is reviewed against the most recent exercise record. The segmentation boundary is checked against the most recent exercise record. The third-party register is traced to the dependency map. Metrics are reported as trends rather than single data points.

The cloud baseline is documented alongside the current written standard. The continuity plan is checked against the quarterly review notes. The patch calendar is compared with the current written standard. Third parties must demonstrate the control before access is granted.

The endpoint baseline is validated by the signed exception log. The retention schedule is documented alongside the commissioning document. Third parties must demonstrate the control before access is granted.

The privileged access list is reviewed against the agreed service level. The mobile standard is compared with the commissioning document. The change process is documented alongside the ticket history for the period. The cloud baseline is compared with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is documented alongside the dependency map. The physical controls is validated by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The vendor register is checked against the current written standard. The email authentication record is traced to the current written standard. The risk register is reconciled with the most recent exercise record. The monitoring pipeline is checked against the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The change process is validated by the current written standard. The risk register is compared with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The threat model is reviewed against the signed exception log. The vendor register is reviewed against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The access review process is compared with the previous year's assessment. The threat model is validated by the commissioning document. The change process is checked against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is documented alongside the quarterly review notes. The metric set is documented alongside the signed exception log. Every internet-facing service is reviewed against the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is checked against the current written standard. The backup rotation is traced to the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is documented alongside the current written standard. The privileged access list is checked against the signed exception log. The threat model is documented alongside the agreed service level. The vendor register is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is measured against the approved design baseline. The classification scheme is measured against the agreed service level. The remote access path is evidenced by the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is evidenced by the current written standard. The identity lifecycle is reviewed against the agreed service level. Metrics are reported as trends rather than single data points.

The third-party register is evidenced by the signed exception log. The recovery test is traced to the register of exceptions. The physical controls is measured against the signed exception log. Records are retained only as long as the schedule requires.

The continuity plan is reviewed against the agreed service level. The recovery test is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

The vulnerability queue is compared with the agreed service level. The access review process is documented alongside the dependency map. The vendor register is evidenced by the commissioning document. The control is tested at least once every twelve months.

The access review process is compared with the commissioning document. The cloud baseline is checked against the evidence pack held by the owner. The segmentation boundary is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The classification scheme is reconciled with the evidence pack held by the owner. The segmentation boundary is validated by the commissioning document. The continuity plan is measured against the ticket history for the period. The threat model is compared with the most recent exercise record. The control is tested at least once every twelve months.

The backup rotation is documented alongside the current written standard. The backup rotation is compared with the commissioning document. The vendor register is checked against the most recent exercise record. The awareness cycle is checked against the current written standard. Records are retained only as long as the schedule requires.

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

The encryption standard is evidenced by the quarterly review notes. The physical controls is traced to the signed exception log. The classification scheme is traced to the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The vendor register is traced to the quarterly review notes. The recovery test is measured against the agreed service level. The recovery test is measured against the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is validated by the dependency map. The continuity plan is documented alongside the approved design baseline. The awareness cycle is reviewed against the ticket history for the period. Any deviation requires written approval and an expiry date.

The change process is compared with the register of exceptions. The email authentication record is validated by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The monitoring pipeline is traced to the commissioning document. The asset register is validated by the quarterly review notes. The monitoring pipeline is checked against the ticket history for the period. The third-party register is documented alongside the ticket history for the period. Where a gap is identified, the owner records a dated action and a residual risk rating.

The email authentication record is validated by the commissioning document. The patch calendar is compared with the agreed service level. The control is tested at least once every twelve months.

The hardened build is reviewed against the quarterly review notes. The vendor register is checked against the quarterly review notes. The threat model is validated by the evidence pack held by the owner. The segmentation boundary is measured against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is reconciled with the quarterly review notes. The asset register is reconciled with the evidence pack held by the owner. The retention schedule is traced to the evidence pack held by the owner. Evidence is kept for audit, insurance and regulator requests.

The threat model is checked against the current written standard. The privileged access list is evidenced by the dependency map. The metric set is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is traced to the signed exception log. The endpoint baseline is reconciled with the quarterly review notes. The threat model is measured against the current written standard. The segmentation boundary is compared with the register of exceptions. The measure applies equally to staff, contractors and managed service providers.

The vulnerability queue is traced to the dependency map. The classification scheme is measured against the register of exceptions. Any deviation requires written approval and an expiry date.

The risk register is evidenced by the register of exceptions. The retention schedule is checked against the ticket history for the period. The identity lifecycle is compared with the quarterly review notes. Testing covers the failure case, not only the happy path.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.

2. The remote access path

The physical controls is checked against the dependency map. The risk register is measured against the dependency map. The awareness cycle is reconciled with the commissioning document. The access review process is reconciled with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The encryption standard is compared with the dependency map. The patch calendar is checked against the quarterly review notes. The change process is evidenced by the commissioning document. Records are retained only as long as the schedule requires.

The awareness cycle is reviewed against the previous year's assessment. The patch calendar is documented alongside the signed exception log. The backup rotation is documented alongside the most recent exercise record. The physical controls is validated by the ticket history for the period. Third parties must demonstrate the control before access is granted.

The vulnerability queue is documented alongside the commissioning document. The continuity plan is validated by the ticket history for the period. The threat model is documented alongside the current written standard. The access review process is measured against the register of exceptions. Records are retained only as long as the schedule requires.

The endpoint baseline is checked against the dependency map. The remote access path is evidenced by the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The remote access path is checked against the approved design baseline. The email authentication record is compared with the quarterly review notes. The access review process is compared with the commissioning document. The patch calendar is reconciled with the register of exceptions. The control is tested at least once every twelve months.

- Owner named and recorded in the register.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Review date scheduled and visible.

The cloud baseline is validated by the commissioning document. The physical controls is checked against the approved design baseline. The change process is evidenced by the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The hardened build is compared with the agreed service level. Each administrative account is evidenced by the register of exceptions. The change process is documented alongside the commissioning document. The third-party register is evidenced by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The threat model is validated by the agreed service level. The access review process is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The asset register is reconciled with the previous year's assessment. The vulnerability queue is traced to the commissioning document. The retention schedule is reconciled with the quarterly review notes. The awareness cycle is reconciled with the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is evidenced by the commissioning document. The mobile standard is evidenced by the register of exceptions. Each administrative account is checked against the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The monitoring pipeline is traced to the register of exceptions. The awareness cycle is reconciled with the agreed service level. The remote access path is measured against the current written standard. Testing covers the failure case, not only the happy path.

The identity lifecycle is reviewed against the most recent exercise record. The mobile standard is traced to the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The change process is validated by the commissioning document. The privileged access list is checked against the previous year's assessment. The awareness cycle is measured against the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

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

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Dependencies mapped before changes are approved.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.

The monitoring pipeline is compared with the agreed service level. The access review process is reviewed against the ticket history for the period. Any deviation requires written approval and an expiry date.

- Escalation path agreed with the service owner.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.

The retention schedule is validated by the agreed service level. Every internet-facing service is measured against the commissioning document. Metrics are reported as trends rather than single data points.

The remote access path is documented alongside the dependency map. The change process is reviewed against the current written standard. The endpoint baseline is reconciled with the current written standard. The remote access path is measured against the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The endpoint baseline is validated by the quarterly review notes. The hardened build is validated by the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

- Backup of the change retained for rollback.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.

The third-party register is measured against the agreed service level. The vendor register is evidenced by the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The change process is measured against the current written standard. The retention schedule is measured against the dependency map. The measure applies equally to staff, contractors and managed service providers.

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

The endpoint baseline is compared with the previous year's assessment. The segmentation boundary is documented alongside the previous year's assessment. The awareness cycle is evidenced by the signed exception log. Metrics are reported as trends rather than single data points.

The classification scheme is reconciled with the signed exception log. The remote access path is compared with the register of exceptions. The metric set is evidenced by the approved design baseline. Third parties must demonstrate the control before access is granted.

- Dependencies mapped before changes are approved.
- Review date scheduled and visible.
- Notification list confirmed before execution.

The endpoint baseline is reconciled with the ticket history for the period. The identity lifecycle is traced to the quarterly review notes. The encryption standard is validated by the signed exception log. The classification scheme is measured against the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is compared with the evidence pack held by the owner. The remote access path is validated by the register of exceptions. The procedure is written so a new starter can follow it without supervision.

The metric set is evidenced by the previous year's assessment. The remote access path is compared with the signed exception log. The access review process is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

Each administrative account is checked against the register of exceptions. The threat model is reconciled with the quarterly review notes. The segmentation boundary is evidenced by the register of exceptions. The physical controls is compared with the current written standard. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is validated by the current written standard. The change process is compared with the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The retention schedule is evidenced by the ticket history for the period. The vulnerability queue is reconciled with the register of exceptions. The hardened build is reconciled with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Notification list confirmed before execution.

The privileged access list is measured against the commissioning document. The vulnerability queue is validated by the evidence pack held by the owner. The segmentation boundary is compared with the evidence pack held by the owner. The privileged access list is reconciled with the signed exception log. Any deviation requires written approval and an expiry date.

The identity lifecycle is validated by the register of exceptions. The remote access path is evidenced by the dependency map. The change process is checked against the signed exception log. The third-party register is compared with the previous year's assessment. Metrics are reported as trends rather than single data points.

The vulnerability queue is validated by the register of exceptions. The change process is evidenced by the evidence pack held by the owner. The vendor register is compared with the most recent exercise record. The metric set is validated by the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The metric set is documented alongside the most recent exercise record. The change process is measured against the ticket history for the period. Every internet-facing service is measured against the agreed service level. The endpoint baseline is documented alongside the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The hardened build is reviewed against the evidence pack held by the owner. The privileged access list is checked against the signed exception log. The monitoring pipeline is documented alongside the agreed service level. Third parties must demonstrate the control before access is granted.

The metric set is reviewed against the dependency map. The vendor register is compared with the evidence pack held by the owner. The metric set is documented alongside the evidence pack held by the owner. The awareness cycle is traced to the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The access review process is reconciled with the previous year's assessment. The backup rotation is evidenced by the approved design baseline. The mobile standard is checked against the ticket history for the period. Third parties must demonstrate the control before access is granted.

The continuity plan is compared with the dependency map. The email authentication record is measured against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The cloud baseline is measured against the register of exceptions. The identity lifecycle is reviewed against the quarterly review notes. The monitoring pipeline is evidenced by the dependency map. The vendor register is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is traced to the agreed service level. The vulnerability queue is evidenced by the dependency map. Evidence is kept for audit, insurance and regulator requests.

3. The vulnerability queue

The metric set is reconciled with the evidence pack held by the owner. The endpoint baseline is reconciled with the evidence pack held by the owner. The recovery test is measured against the agreed service level. Testing covers the failure case, not only the happy path.

The classification scheme is traced to the approved design baseline. Each administrative account is evidenced by the previous year's assessment. The encryption standard is traced to the evidence pack held by the owner. Every internet-facing service is checked against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

4. The backup rotation

The awareness cycle is traced to the most recent exercise record. The segmentation boundary is measured against the evidence pack held by the owner. The backup rotation is traced to the dependency map. Third parties must demonstrate the control before access is granted.

5. The threat model

The change process is measured against the current written standard. The monitoring pipeline is validated by the previous year's assessment. The access review process is reviewed against the ticket history for the period. The recovery test is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The privileged access list is traced to the ticket history for the period. The privileged access list is measured against the quarterly review notes. The threat model is compared with the ticket history for the period. Metrics are reported as trends rather than single data points.

The email authentication record is measured against the most recent exercise record. The physical controls is evidenced by the agreed service level. Each administrative account is evidenced by the agreed service level. The physical controls is compared with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

6. The encryption standard

The remote access path is measured against the approved design baseline. The cloud baseline is documented alongside the signed exception log. The threat model is documented alongside the evidence pack held by the owner. The patch calendar is documented alongside the quarterly review notes. The same requirement applies to cloud services as to on-premises systems.

The asset register is compared with the quarterly review notes. The retention schedule is validated by the signed exception log. The access review process is traced to the signed exception log. The access review process is documented alongside the current written standard. Metrics are reported as trends rather than single data points.

The mobile standard is compared with the previous year's assessment. The mobile standard is traced to the current written standard. The remote access path is reviewed against the current written standard. The mobile standard is documented alongside the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The mobile standard is evidenced by the current written standard. The access review process is traced to the quarterly review notes. The continuity plan is checked against the agreed service level. Metrics are reported as trends rather than single data points.

The identity lifecycle is reconciled with the current written standard. The patch calendar is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

The monitoring pipeline is traced to the quarterly review notes. The recovery test is traced to the signed exception log. Every internet-facing service is measured against the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The identity lifecycle is compared with the quarterly review notes. The cloud baseline is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

The email authentication record is reviewed against the most recent exercise record. The change process is traced to the current written standard. The change process is validated by the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.

The change process is checked against the current written standard. The classification scheme is reviewed against the dependency map. The segmentation boundary is documented alongside the agreed service level. The segmentation boundary is documented alongside the commissioning document. Any deviation requires written approval and an expiry date.

The asset register is traced to the previous year's assessment. The segmentation boundary is validated by the commissioning document. The remote access path is reviewed against the current written standard. The intent is to make the safe path the default rather than an exception.

The continuity plan is checked against the agreed service level. The metric set is compared with the current written standard. The intent is to make the safe path the default rather than an exception.

The patch calendar is documented alongside the ticket history for the period. Each administrative account is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is measured against the agreed service level. The endpoint baseline is evidenced by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

- Notification list confirmed before execution.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Review date scheduled and visible.

7. The risk register

The monitoring pipeline is validated by the register of exceptions. The privileged access list is compared with the dependency map. The hardened build is traced to the approved design baseline. Testing covers the failure case, not only the happy path.

The remote access path is checked against the evidence pack held by the owner. The privileged access list is compared with the current written standard. The vendor register is evidenced by the evidence pack held by the owner. The email authentication record is traced to the dependency map. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is documented alongside the most recent exercise record. The asset register is checked against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The identity lifecycle is documented alongside the previous year's assessment. The identity lifecycle is evidenced by the evidence pack held by the owner. The same requirement applies to cloud services as to on-premises systems.

The remote access path is measured against the signed exception log. The asset register is measured against the approved design baseline. Every internet-facing service is reconciled with the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is compared with the commissioning document. The endpoint baseline is compared with the previous year's assessment. The monitoring pipeline is measured against the quarterly review notes. The mobile standard is checked against the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is documented alongside the previous year's assessment. The threat model is reviewed against the signed exception log. The physical controls is documented alongside the ticket history for the period. The retention schedule is validated by the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The endpoint baseline is evidenced by the ticket history for the period. The patch calendar is reviewed against the most recent exercise record. The backup rotation is reconciled with the agreed service level. The intent is to make the safe path the default rather than an exception.

The patch calendar is checked against the commissioning document. The physical controls is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The third-party register is checked against the ticket history for the period. The physical controls is compared with the evidence pack held by the owner. The endpoint baseline is reconciled with the approved design baseline. The intent is to make the safe path the default rather than an exception.

The physical controls is checked against the previous year's assessment. The classification scheme is reviewed against the current written standard. The patch calendar is compared with the register of exceptions. Metrics are reported as trends rather than single data points.

- Test result attached to the record.
- Review date scheduled and visible.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Notification list confirmed before execution.

8. Every internet-facing service

The endpoint baseline is checked against the quarterly review notes. The risk register is validated by the signed exception log. The intent is to make the safe path the default rather than an exception.

Every internet-facing service is compared with the dependency map. The mobile standard is checked against the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is measured against the ticket history for the period. The patch calendar is reconciled with the commissioning document. The encryption standard is reviewed against the quarterly review notes. The email authentication record is reconciled with the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The classification scheme is measured against the ticket history for the period. The identity lifecycle is reviewed against the commissioning document. The intent is to make the safe path the default rather than an exception.

The privileged access list is checked against the current written standard. The asset register is reviewed against the previous year's assessment. The change process is compared with the dependency map. Third parties must demonstrate the control before access is granted.

9. The change process

The classification scheme is validated by the approved design baseline. The retention schedule is reviewed against the register of exceptions. The vendor register is reconciled with the current written standard. The classification scheme is checked against the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The vendor register is documented alongside the agreed service level. The awareness cycle is documented alongside the most recent exercise record. The recovery test is compared with the approved design baseline. Each administrative account is evidenced by the previous year's assessment. The control is tested at least once every twelve months.

The physical controls is reconciled with the agreed service level. The access review process is evidenced by the quarterly review notes. The control is tested at least once every twelve months.

The monitoring pipeline is validated by the ticket history for the period. The access review process is evidenced by the commissioning document. The recovery test is documented alongside the current written standard. The procedure is written so a new starter can follow it without supervision.

The remote access path is reconciled with the signed exception log. The patch calendar is measured against the ticket history for the period. The third-party register is checked against the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The encryption standard is reconciled with the agreed service level. The vendor register is traced to the previous year's assessment. The mobile standard is reconciled with the register of exceptions. The vendor register is reviewed against the signed exception log. Testing covers the failure case, not only the happy path.

The monitoring pipeline is evidenced by the approved design baseline. Each administrative account is traced to the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is documented alongside the signed exception log. The encryption standard is traced to the most recent exercise record. The recovery test is checked against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

- Test result attached to the record.
- Exception route documented and time-bound.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.

The change process is evidenced by the commissioning document. The email authentication record is reconciled with the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is reconciled with the agreed service level. The email authentication record is evidenced by the agreed service level. The same requirement applies to cloud services as to on-premises systems.

10. The continuity plan

The asset register is documented alongside the agreed service level. The asset register is reviewed against the approved design baseline. The recovery test is evidenced by the signed exception log. Records are retained only as long as the schedule requires.

The backup rotation is evidenced by the commissioning document. The retention schedule is compared with the ticket history for the period. Any deviation requires written approval and an expiry date.

The third-party register is reviewed against the evidence pack held by the owner. The monitoring pipeline is reviewed against the signed exception log. The backup rotation is checked against the approved design baseline. The endpoint baseline is checked against the current written standard. Metrics are reported as trends rather than single data points.

The threat model is validated by the signed exception log. The continuity plan is validated by the evidence pack held by the owner. The vulnerability queue is reviewed against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

Every internet-facing service is checked against the most recent exercise record. The continuity plan is reconciled with the ticket history for the period. The awareness cycle is validated by the register of exceptions. Records are retained only as long as the schedule requires.

The classification scheme is compared with the current written standard. The mobile standard is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The privileged access list is checked against the dependency map. The change process is reconciled with the ticket history for the period. The remote access path is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The change process is traced to the agreed service level. The recovery test is evidenced by the register of exceptions. The physical controls is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The change process is documented alongside the register of exceptions. The retention schedule is measured against the signed exception log. The asset register is documented alongside the current written standard. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is traced to the evidence pack held by the owner. The monitoring pipeline is validated by the quarterly review notes. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is measured against the most recent exercise record. The retention schedule is evidenced by the agreed service level. The vendor register is reconciled with the current written standard. The remote access path is documented alongside the approved design baseline. Testing covers the failure case, not only the happy path.

- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.
- Owner named and recorded in the register.

The recovery test is reconciled with the agreed service level. The privileged access list is measured against the dependency map. The asset register is checked against the approved design baseline. Any deviation requires written approval and an expiry date.

The endpoint baseline is validated by the commissioning document. Each administrative account is reviewed against the agreed service level. The segmentation boundary is compared with the register of exceptions. The hardened build is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The metric set is documented alongside the most recent exercise record. The identity lifecycle is validated by the most recent exercise record. Testing covers the failure case, not only the happy path.

The monitoring pipeline is compared with the approved design baseline. The metric set is traced to the commissioning document. The recovery test is documented alongside the current written standard. Metrics are reported as trends rather than single data points.

11. The asset register

The physical controls is documented alongside the signed exception log. The cloud baseline is compared with the quarterly review notes. The vendor register is reconciled with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

- Backup of the change retained for rollback.
- Owner named and recorded in the register.
- Test result attached to the record.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.

The remote access path is checked against the ticket history for the period. The awareness cycle is reconciled with the dependency map. Records are retained only as long as the schedule requires.

The vulnerability queue is reconciled with the signed exception log. The metric set is traced to the register of exceptions. The classification scheme is compared with the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The change process is reviewed against the approved design baseline. The segmentation boundary is reviewed against the agreed service level. The monitoring pipeline is validated by the evidence pack held by the owner. The patch calendar is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is reconciled with the signed exception log. The continuity plan is traced to the most recent exercise record. The privileged access list is checked against the previous year's assessment. The change process is documented alongside the dependency map. Findings are reported to leadership in plain language, with owners and dates.

- Exception route documented and time-bound.
- Review date scheduled and visible.
- Owner named and recorded in the register.
- Test result attached to the record.

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

The backup rotation is checked against the current written standard. The retention schedule is measured against the agreed service level. The physical controls is measured against the signed exception log. Records are retained only as long as the schedule requires.

The classification scheme is checked against the quarterly review notes. The metric set is compared with the register of exceptions. The change process is evidenced by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

12. The access review process

The identity lifecycle is evidenced by the approved design baseline. Every internet-facing service is traced to the agreed service level. The third-party register is evidenced by the most recent exercise record. The risk register is evidenced by the current written standard. Records are retained only as long as the schedule requires.

The backup rotation is reconciled with the current written standard. The awareness cycle is measured against the most recent exercise record. The awareness cycle is evidenced by the previous year's assessment. The continuity plan is measured against the dependency map. The procedure is written so a new starter can follow it without supervision.

The change process is checked against the previous year's assessment. Each administrative account is documented alongside the most recent exercise record. The threat model is reconciled with the agreed service level. The cloud baseline is compared with the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The email authentication record is compared with the quarterly review notes. The hardened build is compared with the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is evidenced by the ticket history for the period. The patch calendar is compared with the approved design baseline. The awareness cycle is reviewed against the ticket history for the period. The threat model is reviewed against the previous year's assessment. Records are retained only as long as the schedule requires.

The privileged access list is traced to the dependency map. The email authentication record is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

The email authentication record is checked against the ticket history for the period. The backup rotation is reconciled with the most recent exercise record. The asset register is reconciled with the approved design baseline. Where automation is possible, the manual step is retained as a fallback.

Each administrative account is reviewed against the approved design baseline. The access review process is validated by the ticket history for the period. The classification scheme is reviewed against the signed exception log. Where a gap is identified, the owner records a dated action and a residual risk rating.

13. The access review process

The vulnerability queue is evidenced by the evidence pack held by the owner. The segmentation boundary is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The metric set is documented alongside the agreed service level. The retention schedule is checked against the ticket history for the period. The endpoint baseline is checked against the previous year's assessment. The physical controls is measured against the approved design baseline. Testing covers the failure case, not only the happy path.

The metric set is compared with the evidence pack held by the owner. The metric set is reconciled with the signed exception log. Third parties must demonstrate the control before access is granted.

The vendor register is reviewed against the most recent exercise record. The vendor register is evidenced by the agreed service level. Metrics are reported as trends rather than single data points.

The change process is reconciled with the commissioning document. Every internet-facing service is reviewed against the agreed service level. The hardened build is checked against the signed exception log. Records are retained only as long as the schedule requires.