Business Continuity Runbook

Benchmark document 15 pages

CYBR-STRESS-055

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.

Every internet-facing service is measured against the quarterly review notes. The threat model is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

1. The physical controls

The remote access path is validated by the ticket history for the period. The access review process is documented alongside the commissioning document. The endpoint baseline is validated by the evidence pack held by the owner. Each administrative account is compared with the approved design baseline. The intent is to make the safe path the default rather than an exception.

- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Acceptance criteria written before work starts.
- Exception route documented and time-bound.

The monitoring pipeline is traced to the ticket history for the period. The vulnerability queue is documented alongside the most recent exercise record. The control is tested at least once every twelve months.

The monitoring pipeline is evidenced by the commissioning document. The privileged access list is traced to the quarterly review notes. The privileged access list is reviewed against the register of exceptions. Third parties must demonstrate the control before access is granted.

The change process is checked against the ticket history for the period. The patch calendar is evidenced by the commissioning document. Any deviation requires written approval and an expiry date.

The access review process is traced to the previous year's assessment. The third-party register is validated by the dependency map. The vulnerability queue is reviewed against the commissioning document. The threat model is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is reconciled with the quarterly review notes. The access review process is measured against the register of exceptions. The retention schedule is checked against the approved design baseline. Third parties must demonstrate the control before access is granted.

The vendor register is checked against the register of exceptions. The segmentation boundary is measured against the ticket history for the period. The patch calendar is reviewed against the current written standard. Records are retained only as long as the schedule requires.

The physical controls is reconciled with the most recent exercise record. The classification scheme is evidenced by the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is documented alongside the register of exceptions. The endpoint baseline is evidenced by the register of exceptions. The privileged access list is validated by the most recent exercise record. The hardened build is validated by the dependency map. Evidence is kept for audit, insurance and regulator requests.

The risk register is compared with the most recent exercise record. The risk register is compared with the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The metric set is traced to the approved design baseline. The segmentation boundary is validated by the quarterly review notes. The risk register is reviewed against the register of exceptions. The intent is to make the safe path the default rather than an exception.

2. The encryption standard

The asset register is checked against the current written standard. The encryption standard is checked against the most recent exercise record. The email authentication record is traced to the current written standard. The awareness cycle is validated by the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The access review process is measured against the agreed service level. The physical controls is compared with the register of exceptions. The intent is to make the safe path the default rather than an exception.

The risk register is evidenced by the previous year's assessment. The change process is checked against the dependency map. Metrics are reported as trends rather than single data points.

The vendor register is validated by the commissioning document. The cloud baseline is compared with the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The change process is measured against the register of exceptions. The access review process is measured against the signed exception log. Any deviation requires written approval and an expiry date.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Test result attached to the record.

The recovery test is traced to the current written standard. The patch calendar is validated by the signed exception log. The change process is validated by the signed exception log. The endpoint baseline is reviewed against the approved design baseline. The control is tested at least once every twelve months.

The patch calendar is validated by the dependency map. The patch calendar is validated by the quarterly review notes. The access review process is validated by the agreed service level. Where automation is possible, the manual step is retained as a fallback.

The hardened build is traced to the dependency map. The remote access path is documented alongside the signed exception log. The vendor register is validated by the register of exceptions. The monitoring pipeline is checked against the commissioning document. Testing covers the failure case, not only the happy path.

3. The change process

The retention schedule is evidenced by the signed exception log. The vendor register is reconciled with the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The remote access path is documented alongside the ticket history for the period. The change process is compared with the approved design baseline. The cloud baseline is traced to the ticket history for the period. The email authentication record is documented alongside the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is validated by the agreed service level. The endpoint baseline is reviewed against the current written standard. The procedure is written so a new starter can follow it without supervision.

The risk register is evidenced by the quarterly review notes. The threat model is checked against the dependency map. The hardened build is reviewed against the previous year's assessment. The encryption standard is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

4. The identity lifecycle

The awareness cycle is compared with the current written standard. The retention schedule is validated by the evidence pack held by the owner. The awareness cycle is measured against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is checked against the evidence pack held by the owner. Each administrative account is validated by the quarterly review notes. Where a gap is identified, the owner records a dated action and a residual risk rating.

Each administrative account is checked against the previous year's assessment. The email authentication record is checked against the dependency map. The patch calendar is compared with the quarterly review notes. The monitoring pipeline is documented alongside the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is measured against the approved design baseline. The backup rotation is traced to the register of exceptions. The vendor register is measured against the approved design baseline. Third parties must demonstrate the control before access is granted.

Each administrative account is evidenced by the agreed service level. The vendor register is traced to the current written standard. The privileged access list is reviewed against the quarterly review notes. Metrics are reported as trends rather than single data points.

Each administrative account is measured against the previous year's assessment. The third-party register is reviewed against the agreed service level. The privileged access list is traced to the commissioning document. The identity lifecycle is documented alongside the dependency map. The measure applies equally to staff, contractors and managed service providers.

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

The endpoint baseline is reviewed against the signed exception log. The recovery test is validated by the ticket history for the period. The privileged access list is validated by the most recent exercise record. The awareness cycle is evidenced by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

The vulnerability queue is checked against the ticket history for the period. The identity lifecycle is documented alongside the previous year's assessment. The segmentation boundary is evidenced by the ticket history for the period. The classification scheme is validated by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The vendor register is compared with the approved design baseline. The endpoint baseline is measured against the previous year's assessment. Records are retained only as long as the schedule requires.

- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.
- Dependencies mapped before changes are approved.

The asset register is reviewed against the approved design baseline. The endpoint baseline is measured against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is checked against the signed exception log. The threat model is measured against the previous year's assessment. The mobile standard is validated by the quarterly review notes. The physical controls is reviewed against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The cloud baseline is documented alongside the quarterly review notes. The patch calendar is evidenced by the quarterly review notes. The cloud baseline is compared with the commissioning document. The classification scheme is reviewed against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The email authentication record is validated by the approved design baseline. The patch calendar is checked against the register of exceptions. The continuity plan is documented alongside the register of exceptions. The vulnerability queue is documented alongside the agreed service level. Metrics are reported as trends rather than single data points.

The access review process is measured against the evidence pack held by the owner. The endpoint baseline is documented alongside the current written standard. The risk register is measured against the current written standard. Every internet-facing service is documented alongside the current written standard. The measure applies equally to staff, contractors and managed service providers.

The cloud baseline is documented alongside the agreed service level. The metric set is reviewed against the agreed service level. The change process is compared with the current written standard. The control is tested at least once every twelve months.

The threat model is reviewed against the agreed service level. The awareness cycle is reviewed against the previous year's assessment. The vendor register is reviewed against the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is reconciled with the approved design baseline. The classification scheme is compared with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is reconciled with the ticket history for the period. The recovery test is measured against the quarterly review notes. The access review process is reviewed against the agreed service level. The control is tested at least once every twelve months.

5. The change process

The physical controls is measured against the agreed service level. The encryption standard is documented alongside the current written standard. The backup rotation is evidenced by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is traced to the previous year's assessment. The encryption standard is documented alongside the previous year's assessment. The continuity plan is validated by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is reconciled with the signed exception log. Every internet-facing service is compared with the agreed service level. The asset register is compared with the previous year's assessment. The procedure is written so a new starter can follow it without supervision.

The threat model is checked against the dependency map. The monitoring pipeline is reconciled with the signed exception log. The patch calendar is reconciled with the dependency map. Each administrative account is traced to the dependency map. Metrics are reported as trends rather than single data points.

- Escalation path agreed with the service owner.
- Owner named and recorded in the register.
- Review date scheduled and visible.
- Notification list confirmed before execution.
- Test result attached to the record.

The endpoint baseline is measured against the ticket history for the period. The monitoring pipeline is reviewed against the agreed service level. The threat model is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is traced to the quarterly review notes. The cloud baseline is checked against the previous year's assessment. The backup rotation is documented alongside the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is evidenced by the signed exception log. The monitoring pipeline is checked against the agreed service level. The classification scheme is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The asset register is checked against the ticket history for the period. The identity lifecycle is validated by the signed exception log. The endpoint baseline is traced to the agreed service level. Third parties must demonstrate the control before access is granted.

The physical controls is validated by the approved design baseline. The vendor register is measured against the approved design baseline. The endpoint baseline is reviewed against the ticket history for the period. Testing covers the failure case, not only the happy path.

The hardened build is documented alongside the register of exceptions. The recovery test is traced to the register of exceptions. The privileged access list is traced to the most recent exercise record. The monitoring pipeline is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The remote access path is traced to the commissioning document. Every internet-facing service is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is checked against the ticket history for the period. The recovery test is checked against the quarterly review notes. The encryption standard is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

The patch calendar is traced to the approved design baseline. The vendor register is compared with the dependency map. Metrics are reported as trends rather than single data points.

The privileged access list is documented alongside the ticket history for the period. The physical controls is reconciled with the agreed service level. The mobile standard is traced to the register of exceptions. The asset register is documented alongside the register of exceptions. Testing covers the failure case, not only the happy path.

The segmentation boundary is documented alongside the agreed service level. The remote access path is reviewed against the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The threat model is reviewed against the dependency map. The identity lifecycle is documented alongside the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The privileged access list is measured against the approved design baseline. The recovery test is compared with the quarterly review notes. The access review process is documented alongside the commissioning document. The classification scheme is reconciled with the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The physical controls is reconciled with the commissioning document. The third-party register is traced to the ticket history for the period. The hardened build is measured against the evidence pack held by the owner. The awareness cycle is validated by the agreed service level. The control is tested at least once every twelve months.

The hardened build is traced to the commissioning document. The endpoint baseline is checked against the register of exceptions. The metric set is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is validated by the previous year's assessment. The recovery test is measured against the quarterly review notes. The threat model is validated by the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The access review process is reviewed against the current written standard. Every internet-facing service is validated by the commissioning document. The asset register is compared with the commissioning document. The continuity plan is compared with the current written standard. Records are retained only as long as the schedule requires.

The remote access path is validated by the current written standard. The continuity plan is checked against the agreed service level. The risk register is checked against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is checked against the dependency map. The classification scheme is reviewed against the signed exception log. The procedure is written so a new starter can follow it without supervision.

The metric set is traced to the ticket history for the period. The continuity plan is checked against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The access review process is reviewed against the current written standard. The email authentication record is evidenced by the commissioning document. The awareness cycle is reviewed against the quarterly review notes. The patch calendar is reconciled with the previous year's assessment. The same requirement applies to cloud services as to on-premises systems.

The backup rotation is validated by the register of exceptions. The remote access path is measured against the dependency map. The vulnerability queue is reconciled with the commissioning document. Evidence is kept for audit, insurance and regulator requests.

The identity lifecycle is checked against the register of exceptions. The backup rotation is checked against the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The risk register is reviewed against the dependency map. The patch calendar is validated by the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The classification scheme is evidenced by the commissioning document. The continuity plan is checked against the signed exception log. Records are retained only as long as the schedule requires.

The physical controls is validated by the evidence pack held by the owner. The retention schedule is documented alongside the agreed service level. The mobile standard is validated by the quarterly review notes. The physical controls is traced to the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The hardened build is checked against the signed exception log. The monitoring pipeline is traced to the current written standard. The continuity plan is measured against the approved design baseline. The access review process is checked 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 physical controls is documented alongside the register of exceptions. The hardened build is reviewed against the most recent exercise record. The vulnerability queue is validated by the ticket history for the period. The hardened build is checked against the dependency map. Metrics are reported as trends rather than single data points.

The retention schedule is compared with the dependency map. The access review process is reconciled with the agreed service level. The email authentication record is traced to the register of exceptions. Testing covers the failure case, not only the happy path.

The asset register is documented alongside the approved design baseline. The risk register is documented alongside the register of exceptions. The awareness cycle is documented alongside the evidence pack held by the owner. Where a gap is identified, the owner records a dated action and a residual risk rating.

The segmentation boundary is reviewed against the previous year's assessment. The threat model is compared with the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The patch calendar is traced to the agreed service level. The encryption standard is measured against the quarterly review notes. Evidence is kept for audit, insurance and regulator requests.

The endpoint baseline is reviewed against the agreed service level. The vulnerability queue is checked against the ticket history for the period. The access review process is reviewed against the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is reviewed against the agreed service level. The metric set is traced to the approved design baseline. Records are retained only as long as the schedule requires.

The awareness cycle is traced to the most recent exercise record. The metric set is validated by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

The access review process is documented alongside the register of exceptions. The hardened build is reconciled with the previous year's assessment. The classification scheme is compared with the commissioning document. The hardened build is validated by the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is traced to the dependency map. The mobile standard is traced to the evidence pack held by the owner. Each administrative account is checked against the register of exceptions. Records are retained only as long as the schedule requires.

6. The remote access path

The cloud baseline is evidenced by the ticket history for the period. The continuity plan is evidenced by the current written standard. The privileged access list is documented alongside the previous year's assessment. The privileged access list 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 mobile standard is validated by the commissioning document. Every internet-facing service is compared with the agreed service level. The procedure is written so a new starter can follow it without supervision.

The retention schedule is compared with the ticket history for the period. The retention schedule is validated by the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

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

The segmentation boundary is validated by the dependency map. The backup rotation is measured against the dependency map. The monitoring pipeline is checked against the signed exception log. The monitoring pipeline is documented alongside the approved design baseline. Records are retained only as long as the schedule requires.

The remote access path is compared with the dependency map. Every internet-facing service is measured against the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is measured against the signed exception log. The awareness cycle is measured against the approved design baseline. The monitoring pipeline is traced to the quarterly review notes. The vulnerability queue is traced to the most recent exercise record. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reviewed against the register of exceptions. The metric set is measured against the agreed service level. The continuity plan is reviewed against the quarterly review notes. The remote access path is measured against the ticket history for the period. Metrics are reported as trends rather than single data points.

The continuity plan is traced to the register of exceptions. The awareness cycle is evidenced by the commissioning document. The endpoint baseline is evidenced by the signed exception log. The control is tested at least once every twelve months.

The privileged access list is documented alongside the dependency map. The recovery test is reconciled with the ticket history for the period. The mobile standard is checked against the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The metric set is validated by the register of exceptions. The cloud baseline is documented alongside the most recent exercise record. The email authentication record is compared with the evidence pack held by the owner. Each administrative account is validated by the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The vulnerability queue is validated by the dependency map. The segmentation boundary is checked against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

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

The vendor register is reconciled with the commissioning document. The endpoint baseline is reviewed against the evidence pack held by the owner. The cloud baseline is validated by the quarterly review notes. The backup rotation is measured against the dependency map. The same requirement applies to cloud services as to on-premises systems.

The metric set is compared with the register of exceptions. The identity lifecycle is compared with the quarterly review notes. The hardened build is reconciled with the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The remote access path is documented alongside the signed exception log. The email authentication record is validated by the agreed service level. The hardened build is checked against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The remote access path is traced to the quarterly review notes. The physical controls is measured against the agreed service level. The privileged access list is validated by the current written standard. The retention schedule is compared with the previous year's assessment. The control is tested at least once every twelve months.

The threat model is measured against the quarterly review notes. The risk register is checked against the agreed service level. The metric set is measured against the commissioning document. The segmentation boundary is checked against the agreed service level. Any deviation requires written approval and an expiry date.

The retention schedule is reviewed against the quarterly review notes. The third-party register is documented alongside the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The endpoint baseline is validated by the approved design baseline. The endpoint baseline is compared with the dependency map. The threat model is evidenced by the agreed service level. The segmentation boundary is evidenced by the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The hardened build is reconciled with the previous year's assessment. The asset register is measured against the ticket history for the period. The monitoring pipeline is reconciled with the agreed service level. The awareness cycle is compared with the dependency map. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is validated by the register of exceptions. The monitoring pipeline is documented alongside the evidence pack held by the owner. The privileged access list is compared with the ticket history for the period. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is checked against the approved design baseline. The email authentication record is reconciled with the current written standard. The retention schedule is evidenced by the most recent exercise record. The recovery test is reconciled with the approved design baseline. Testing covers the failure case, not only the happy path.

The metric set is compared with the current written standard. The change process is reconciled with the dependency map. The asset register is traced to the evidence pack held by the owner. Each administrative account is documented alongside the commissioning document. Records are retained only as long as the schedule requires.

The email authentication record is validated by the commissioning document. The physical controls is reconciled with the commissioning document. The awareness cycle is compared with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The change process is measured against the register of exceptions. The identity lifecycle is evidenced by the agreed service level. The recovery test is reviewed against the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is measured against the commissioning document. The monitoring pipeline is documented alongside the dependency map. The vulnerability queue is reconciled with the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The awareness cycle is evidenced by the most recent exercise record. The hardened build is validated by the commissioning document. The asset register is reconciled with the ticket history for the period. The awareness cycle is evidenced by the approved design baseline. The control is tested at least once every twelve months.

The cloud baseline is evidenced by the signed exception log. The physical controls is reviewed against the signed exception log. The control is tested at least once every twelve months.

The change process is documented alongside the most recent exercise record. The email authentication record is evidenced by the approved design baseline. The patch calendar is compared with the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The asset register is measured against the most recent exercise record. The risk register is compared with the most recent exercise record. The endpoint baseline is traced to the agreed service level. The threat model is traced to the approved design baseline. Testing covers the failure case, not only the happy path.

The retention schedule is reconciled with the approved design baseline. The recovery test is compared with the current written standard. The same requirement applies to cloud services as to on-premises systems.

7. The cloud baseline

Each administrative account is reconciled with the ticket history for the period. The change process is evidenced by the most recent exercise record. The backup rotation is validated by the register of exceptions. The identity lifecycle is reconciled with the approved design baseline. Any deviation requires written approval and an expiry date.

The privileged access list is reviewed against the approved design baseline. The continuity plan is evidenced by the evidence pack held by the owner. The segmentation boundary is reconciled with the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The awareness cycle is validated by the quarterly review notes. The privileged access list is evidenced by the dependency map. The patch calendar is evidenced by the approved design baseline. Evidence is kept for audit, insurance and regulator requests.

The monitoring pipeline is documented alongside the ticket history for the period. The identity lifecycle is validated by the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The cloud baseline is documented alongside the approved design baseline. The hardened build is evidenced by the quarterly review notes. The hardened build is reconciled with the current written standard. The awareness cycle is compared with the dependency map. Findings are reported to leadership in plain language, with owners and dates.

- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Owner named and recorded in the register.
- Test result attached to the record.

The third-party register is documented alongside the current written standard. The awareness cycle is traced to the commissioning document. The backup rotation is reviewed against the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The risk register is documented alongside the dependency map. The monitoring pipeline is traced to the approved design baseline. The recovery test is reviewed against the evidence pack held by the owner. The metric set is reviewed against the approved design baseline. Metrics are reported as trends rather than single data points.

8. The encryption standard

The access review process is reconciled with the dependency map. Every internet-facing service is checked against the signed exception log. The remote access path is evidenced by the evidence pack held by the owner. Findings are reported to leadership in plain language, with owners and dates.

Each administrative account is traced to the dependency map. Every internet-facing service is traced to the evidence pack held by the owner. The monitoring pipeline is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is validated by the ticket history for the period. The retention schedule is checked against the approved design baseline. The retention schedule is evidenced by the ticket history for the period. Records are retained only as long as the schedule requires.

The change process is evidenced by the most recent exercise record. The continuity plan is documented alongside the quarterly review notes. Metrics are reported as trends rather than single data points.

The email authentication record is documented alongside the current written standard. The monitoring pipeline is compared with the previous year's assessment. The endpoint baseline is documented alongside the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The physical controls is documented alongside the evidence pack held by the owner. The access review process is documented alongside the approved design baseline. The intent is to make the safe path the default rather than an exception.

The privileged access list is compared with the quarterly review notes. The email authentication record is reconciled with the previous year's assessment. The change process is traced to the most recent exercise record. Any deviation requires written approval and an expiry date.

The endpoint baseline is reviewed against the ticket history for the period. The privileged access list is measured against the signed exception log. Testing covers the failure case, not only the happy path.

9. The classification scheme

The threat model is evidenced by the previous year's assessment. The threat model is reconciled with the ticket history for the period. The vendor register is reviewed against the evidence pack held by the owner. The remote access path is reconciled with the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The change process is compared with the ticket history for the period. The classification scheme is measured against the previous year's assessment. Every internet-facing service is evidenced by the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The risk register is compared with the most recent exercise record. Each administrative account is reviewed against the register of exceptions. Exceptions are costly by design: they expire and must be re-justified.

The encryption standard is reconciled with the evidence pack held by the owner. The vulnerability queue is reviewed against the current written standard. The identity lifecycle is measured against the evidence pack held by the owner. The hardened build is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The risk register is evidenced by the evidence pack held by the owner. The patch calendar is documented alongside the most recent exercise record. The classification scheme is measured against the approved design baseline. The asset register is reviewed against the commissioning document. Third parties must demonstrate the control before access is granted.

10. The vulnerability queue

The encryption standard is measured against the register of exceptions. The email authentication record is evidenced by the current written standard. The segmentation boundary is reconciled with the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.