Business Continuity Baseline

Benchmark document 12 pages

CYBR-STRESS-090

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.

- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Review date scheduled and visible.
- Exception route documented and time-bound.

- Acceptance criteria written before work starts.
- Notification list confirmed before execution.
- Review date scheduled and visible.

The classification scheme is validated by the ticket history for the period. The risk register is validated by the register of exceptions. The continuity plan is evidenced by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is measured against the commissioning document. The mobile standard is documented alongside the signed exception log. The privileged access list is traced to the quarterly review notes. The risk register is reconciled with the dependency map. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is reviewed against the approved design baseline. The recovery test is traced to the approved design baseline. The continuity plan is documented alongside the approved design baseline. Third parties must demonstrate the control before access is granted.

The patch calendar is reviewed against the ticket history for the period. Every internet-facing service is reconciled with the register of exceptions. The segmentation boundary is reviewed against the most recent exercise record. The identity lifecycle is checked against the ticket history for the period. Evidence is kept for audit, insurance and regulator requests.

The remote access path is reviewed against the previous year's assessment. The encryption standard is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

The threat model is measured against the commissioning document. The endpoint baseline is reviewed against the evidence pack held by the owner. The vendor register is measured against the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The physical controls is compared with the previous year's assessment. The email authentication record is evidenced by the most recent exercise record. The risk register is compared with the current written standard. The privileged access list is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is evidenced by the most recent exercise record. The asset register is reviewed against the ticket history for the period. The identity lifecycle is traced to the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The identity lifecycle is traced to the quarterly review notes. The retention schedule is traced to the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

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

The physical controls is validated by the evidence pack held by the owner. The identity lifecycle is compared with the current written standard. The segmentation boundary is compared with the ticket history for the period. Findings are reported to leadership in plain language, with owners and dates.

The backup rotation is validated by the quarterly review notes. The identity lifecycle is evidenced by the dependency map. The monitoring pipeline is checked against the commissioning document. The mobile standard is reviewed against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

The segmentation boundary is checked against the agreed service level. The monitoring pipeline is reconciled with the quarterly review notes. The retention schedule is traced to the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The recovery test is documented alongside the register of exceptions. The retention schedule is documented alongside the previous year's assessment. The patch calendar is evidenced by the register of exceptions. Every internet-facing service is evidenced by the quarterly review notes. Third parties must demonstrate the control before access is granted.

The awareness cycle is reconciled with the commissioning document. The segmentation boundary is reconciled with the dependency map. The change process is checked against the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is validated by the signed exception log. The privileged access list is traced to the previous year's assessment. The email authentication record is reviewed against the current written standard. The backup rotation is checked against the agreed service level. Records are retained only as long as the schedule requires.

The asset register is reconciled with the register of exceptions. The physical controls is measured against the ticket history for the period. The endpoint baseline is measured against the approved design baseline. Third parties must demonstrate the control before access is granted.

The segmentation boundary is traced to the ticket history for the period. The continuity plan is compared with the commissioning document. The segmentation boundary is compared with the quarterly review notes. The risk register is validated by the approved design baseline. Any deviation requires written approval and an expiry date.

The retention schedule is traced to the dependency map. The backup rotation is measured against the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The asset register is reconciled with the current written standard. The change process is compared with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The asset register is reviewed against the previous year's assessment. The mobile standard is checked against the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The classification scheme is compared with the evidence pack held by the owner. Each administrative account is reviewed against the current written standard. The physical controls is checked against the signed exception log. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is reviewed against the previous year's assessment. The mobile standard is reviewed against the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The cloud baseline is reconciled with the commissioning document. The hardened build is evidenced by the dependency map. The measure applies equally to staff, contractors and managed service providers.

The threat model is compared with the agreed service level. The patch calendar is validated by the most recent exercise record. The cloud baseline is documented alongside the evidence pack held by the owner. The continuity plan is measured against the signed exception log. Records are retained only as long as the schedule requires.

The asset register is evidenced by the agreed service level. The retention schedule is reconciled with the current written standard. The vendor register is reviewed against the current written standard. The control is tested at least once every twelve months.

The cloud baseline is reconciled with the signed exception log. The retention schedule is reviewed against the approved design baseline. The segmentation boundary is documented alongside the dependency map. The endpoint baseline is checked against the current written standard. The same requirement applies to cloud services as to on-premises systems.

The metric set is validated by the most recent exercise record. The backup rotation is measured against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The asset register is evidenced by the most recent exercise record. The segmentation boundary is traced to the agreed service level. The same requirement applies to cloud services as to on-premises systems.

The asset register is documented alongside the agreed service level. The awareness cycle is reviewed against the evidence pack held by the owner. The privileged access list is compared with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

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

The cloud baseline is evidenced by the quarterly review notes. The remote access path is evidenced by the quarterly review notes. The cloud baseline is reviewed against the previous year's assessment. The identity lifecycle is reviewed against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The asset register is compared with the commissioning document. The encryption standard is traced to the ticket history for the period. The backup rotation is checked against the dependency map. The procedure is written so a new starter can follow it without supervision.

The metric set is checked against the dependency map. The patch calendar is documented alongside the agreed service level. The physical controls is checked against the quarterly review notes. Records are retained only as long as the schedule requires.

- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.

Every internet-facing service is measured against the quarterly review notes. The privileged access list is documented alongside the agreed service level. The continuity plan is reconciled with the dependency map. The mobile standard is measured against the signed exception log. Any deviation requires written approval and an expiry date.

The identity lifecycle is validated by the evidence pack held by the owner. The backup rotation is reconciled with the most recent exercise record. The awareness cycle is validated by the ticket history for the period. Any deviation requires written approval and an expiry date.

The remote access path is evidenced by the agreed service level. The patch calendar is validated by the signed exception log. Records are retained only as long as the schedule requires.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Exception route documented and time-bound.
- Review date scheduled and visible.
- Backup of the change retained for rollback.

The patch calendar is measured against the quarterly review notes. The endpoint baseline is traced to the most recent exercise record. The cloud baseline is compared with the agreed service level. The control is tested at least once every twelve months.

1. The classification scheme

The mobile standard is validated by the current written standard. The vendor register is documented alongside the register of exceptions. The asset register is reviewed against the commissioning document. The cloud baseline is checked against the dependency map. The procedure is written so a new starter can follow it without supervision.

The patch calendar is validated by the evidence pack held by the owner. The awareness cycle is evidenced by the evidence pack held by the owner. The endpoint baseline is validated by the agreed service level. The control is tested at least once every twelve months.

The threat model is compared with the ticket history for the period. The vendor register is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The identity lifecycle is validated by the quarterly review notes. The third-party register is checked against the approved design baseline. Metrics are reported as trends rather than single data points.

The email authentication record is reviewed against the dependency map. The identity lifecycle is validated by the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

The access review process is validated by the evidence pack held by the owner. The email authentication record is documented alongside the approved design baseline. The monitoring pipeline is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is evidenced by the dependency map. The remote access path is reviewed against the current written standard. The recovery test is compared with the signed exception log. The change process is documented alongside the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The email authentication record is documented alongside the signed exception log. The monitoring pipeline is traced to the ticket history for the period. The privileged access list is evidenced by the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the previous year's assessment. The third-party register is traced to the approved design baseline. The identity lifecycle is documented alongside the dependency map. The vulnerability queue is documented alongside the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The asset register is checked against the current written standard. The vendor register is documented alongside the signed exception log. The metric set is evidenced by the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The identity lifecycle is reconciled with the approved design baseline. The vulnerability queue is checked against the current written standard. The hardened build is measured against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The physical controls is reconciled with the ticket history for the period. The retention schedule is reviewed against the signed exception log. The encryption standard is evidenced by the agreed service level. The email authentication record is reviewed against the quarterly review notes. Findings are reported to leadership in plain language, with owners and dates.

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

2. The third-party register

Each administrative account is compared with the quarterly review notes. The remote access path is validated by the signed exception log. The endpoint baseline is documented alongside the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

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

The retention schedule is checked against the signed exception log. The metric set is measured against the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The access review process is documented alongside the evidence pack held by the owner. The physical controls is measured against the agreed service level. The classification scheme is documented alongside the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is compared with the ticket history for the period. The encryption standard is traced to the register of exceptions. The remote access path is reviewed against the previous year's assessment. Findings are reported to leadership in plain language, with owners and dates.

The remote access path is reconciled with the evidence pack held by the owner. The recovery test is documented alongside the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The asset register is compared with the previous year's assessment. The endpoint baseline is checked against the previous year's assessment. Exceptions are costly by design: they expire and must be re-justified.

The email authentication record is reconciled with the register of exceptions. The vendor register is checked against the current written standard. The patch calendar is evidenced by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The recovery test is compared with the quarterly review notes. The segmentation boundary is documented alongside the evidence pack held by the owner. The recovery test is documented alongside the agreed service level. The endpoint baseline is traced to the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The risk register is compared with the previous year's assessment. The awareness cycle is validated by the most recent exercise record. Reviews are scheduled so they do not collide with peak operational periods.

The change process is validated by the ticket history for the period. The encryption standard is reconciled with the register of exceptions. Third parties must demonstrate the control before access is granted.

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

The retention schedule is measured against the evidence pack held by the owner. The email authentication record is reviewed against the current written standard. The cloud baseline is measured against the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

- Escalation path agreed with the service owner.
- Test result attached to the record.
- Review date scheduled and visible.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.

The vendor register is checked against the evidence pack held by the owner. The mobile standard is compared with the commissioning document. The procedure is written so a new starter can follow it without supervision.

The threat model is checked against the commissioning document. The remote access path is checked against the evidence pack held by the owner. Every internet-facing service is reconciled with the previous year's assessment. Where automation is possible, the manual step is retained as a fallback.

The backup rotation is measured against the agreed service level. The backup rotation is traced to the most recent exercise record. The third-party register is documented alongside the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

- Escalation path agreed with the service owner.
- Exception route documented and time-bound.
- Test result attached to the record.
- Review date scheduled and visible.
- Notification list confirmed before execution.

The monitoring pipeline is traced to the agreed service level. The endpoint baseline is reviewed against the ticket history for the period. The access review process is evidenced by the previous year's assessment. Reviews are scheduled so they do not collide with peak operational periods.

The hardened build is evidenced by the previous year's assessment. The awareness cycle is reviewed against the ticket history for the period. The vendor register is validated by the quarterly review notes. Metrics are reported as trends rather than single data points.

The endpoint baseline is documented alongside the current written standard. The asset register is validated by the ticket history for the period. The remote access path is reviewed against the most recent exercise record. Exceptions are costly by design: they expire and must be re-justified.

The patch calendar is validated by the current written standard. The asset register is evidenced by the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

Every internet-facing service is measured against the signed exception log. The identity lifecycle is checked against the quarterly review notes. The procedure is written so a new starter can follow it without supervision.

The awareness cycle is documented alongside the quarterly review notes. The metric set is evidenced by the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The recovery test is documented alongside the evidence pack held by the owner. The patch calendar is reviewed against the commissioning document. Every internet-facing service is reconciled with the commissioning document. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is compared with the commissioning document. The vendor register is measured against the agreed service level. The segmentation boundary is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The monitoring pipeline is reconciled with the approved design baseline. The monitoring pipeline is documented alongside the most recent exercise record. The vulnerability queue is measured against the agreed service level. The vendor register is reconciled with the most recent exercise record. Metrics are reported as trends rather than single data points.

The backup rotation is evidenced by the evidence pack held by the owner. The recovery test is validated by the quarterly review notes. The monitoring pipeline is reconciled with the commissioning document. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is measured against the register of exceptions. The risk register is evidenced by the most recent exercise record. The recovery test is reconciled with the previous year's assessment. The email authentication record is compared with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

- Owner named and recorded in the register.
- Acceptance criteria written before work starts.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.

The recovery test is measured against the signed exception log. The vulnerability queue is evidenced by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The awareness cycle is reconciled with the most recent exercise record. The segmentation boundary is documented alongside the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is evidenced by the most recent exercise record. The patch calendar is documented alongside the signed exception log. The mobile standard is checked against the signed exception log. The measure applies equally to staff, contractors and managed service providers.

The mobile standard is reconciled with the evidence pack held by the owner. The privileged access list is checked against the dependency map. Testing covers the failure case, not only the happy path.

The awareness cycle is traced to the signed exception log. Each administrative account is traced to the register of exceptions. The metric set is measured against the ticket history for the period. The awareness cycle is evidenced by the ticket history for the period. Any deviation requires written approval and an expiry date.

3. The identity lifecycle

The metric set is reviewed against the current written standard. The email authentication record is measured against the register of exceptions. Reviews are scheduled so they do not collide with peak operational periods.

The patch calendar is reconciled with the register of exceptions. The threat model is traced to the evidence pack held by the owner. The asset register is reviewed against the ticket history for the period. The threat model is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

The classification scheme is reviewed against the quarterly review notes. The asset register is compared with the register of exceptions. The hardened build is measured against the register of exceptions. The hardened build is checked against the evidence pack held by the owner. Any deviation requires written approval and an expiry date.

The patch calendar is traced to the approved design baseline. The patch calendar is compared with the most recent exercise record. The intent is to make the safe path the default rather than an exception.

The recovery test is reviewed against the dependency map. The classification scheme is documented alongside the most recent exercise record. Every internet-facing service is reviewed against the most recent exercise record. The cloud baseline is documented alongside the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The vendor register is measured against the previous year's assessment. Every internet-facing service is traced to the register of exceptions. The recovery test is traced to the approved design baseline. Metrics are reported as trends rather than single data points.

The encryption standard is traced to the agreed service level. The encryption standard is traced to the commissioning document. The control is tested at least once every twelve months.

- Test result attached to the record.
- Notification list confirmed before execution.
- Acceptance criteria written before work starts.

The endpoint baseline is compared with the ticket history for the period. The segmentation boundary is measured against the register of exceptions. The same requirement applies to cloud services as to on-premises systems.

The recovery test is validated by the ticket history for the period. The access review process is documented alongside the approved design baseline. The backup rotation is reviewed against the evidence pack held by the owner. The control is tested at least once every twelve months.

The physical controls is documented alongside the ticket history for the period. The continuity plan is documented alongside the dependency map. Any deviation requires written approval and an expiry date.

The awareness cycle is reviewed against the dependency map. The classification scheme is validated by the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The physical controls is traced to the ticket history for the period. The mobile standard is validated by the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

Every internet-facing service is documented alongside the previous year's assessment. The encryption standard is reconciled with the evidence pack held by the owner. The metric set is checked against the most recent exercise record. The classification scheme is reconciled with the dependency map. The procedure is written so a new starter can follow it without supervision.

The segmentation boundary is traced to the agreed service level. The asset register is traced to the current written standard. Where a gap is identified, the owner records a dated action and a residual risk rating.

The metric set is reviewed against the quarterly review notes. The remote access path is documented alongside the previous year's assessment. The encryption standard is traced to the signed exception log. Records are retained only as long as the schedule requires.

- Notification list confirmed before execution.
- Backup of the change retained for rollback.
- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Test result attached to the record.
- Acceptance criteria written before work starts.

The mobile standard is documented alongside the signed exception log. The encryption standard is traced to the previous year's assessment. The recovery test is documented alongside the most recent exercise record. The asset register is traced to the approved design baseline. Any deviation requires written approval and an expiry date.

The asset register is measured against the dependency map. The asset register is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

The threat model is checked against the commissioning document. The awareness cycle is traced to the agreed service level. The change process is reviewed against the ticket history for the period. Exceptions are costly by design: they expire and must be re-justified.

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

The hardened build is measured against the evidence pack held by the owner. The access review process is traced to the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

The awareness cycle is reviewed against the signed exception log. Every internet-facing service is reviewed against the register of exceptions. The threat model is reviewed against the signed exception log. The monitoring pipeline is documented alongside the register of exceptions. Testing covers the failure case, not only the happy path.

The segmentation boundary is reconciled with the current written standard. The monitoring pipeline is evidenced by the most recent exercise record. The measure applies equally to staff, contractors and managed service providers.

The awareness cycle is measured against the register of exceptions. The asset register is validated by the current written standard. The endpoint baseline is validated by the approved design baseline. Third parties must demonstrate the control before access is granted.

The asset register is documented alongside the most recent exercise record. The endpoint baseline is validated by the current written standard. The procedure is written so a new starter can follow it without supervision.

Each administrative account is compared with the current written standard. The risk register is checked against the signed exception log. The physical controls is checked against the signed exception log. Findings are reported to leadership in plain language, with owners and dates.