ACME Corporation

Business Continuity & Disaster Recovery | Version 1.0

Policy

Public

Effective: July 6, 2026

Approved By: Amanda Ates

Last Reviewed: July 6, 2026

Table of Contents

- 0 Description 4
- 1.0 Business Continuity 4
- 1.1 Business Continuity Plan 4
- 1.2 Planning Contents 4
- 1.3 Plan Roles and Responsibilities 4
- 1.4 Plan Ownership 4
- 1.5 Plan Distribution 5
- 1.6 Plan Storage 5
- 1.7 Plan Security Requirements 5
- 1.8 Critical Business Processes 5
- 1.9 Identifying Events 5
- 1.10 Risk Assessments 5
- 1.11 Risk Assessment Results 6
- 1.12 Integrated Security 6
- 1.13 Business Impact Analysis 6
- 1.14 System Changes 7
- 1.15 Temporary Operational Procedures 7
- 1.16 Contingency Program 7
- 1.17 Alternative Site Agreements 7
- 1.18 Alternate Site Distances 8
- 1.19 Emergency Power and Telecommunications 8
- 1.20 Alternate Telecommunications 8
- 1.21 Emergency and Fallback Procedures 8
- 1.22 Service Provider Fallback Arrangements 8
- 1.23 New Requirements 9
- 2.0 Disaster Recovery 9
- 2.1 Restoration 9
- 2.2 Backups 9
- 2.3 Backup Definitions 9
- 2.4 Backup Schedule 10
- 2.5 Sensitive Data 10
- 2.6 Automated Tools 10
- 2.7 Backup Testing 10

- 2.8 BYOD Backup Roles 11
- 2.9 Third-Party Backup Services 11
- 2.10 Backup Storage 11
- 2.11 Backup Copies 11
- 2.12 Backup Retention 11
- 2.13 Server Movement 12
- 2.14 Backup Storage Logging 12
- 2.15 Inventory Records 12
- **Procedures Appendix 13**
- Alternate Site & Continuity Infrastructure 13
- Backup Procedure 13
- Business Continuity Plan Development & Maintenance 14
- Disaster Recovery & Restoration 14
- Risk Assessment & Business Impact Analysis (BIA) 15
- **Release and Review History 16**

0 Description

A business continuity policy is the set of standards and guidelines an organization enforces to ensure resilience and proper risk management. Business continuity policies vary by organization and industry and require periodic updates as technologies evolve and business risks change.

1.0 Business Continuity

1.1 Business Continuity Plan

At least one business continuity plan must be formally documented for each business unit which describes the approach for continuity, ensuring the minimum approach to maintain information or information asset availability and security, including an escalation plan and the conditions for its activation.

HITRUST 1666.12d1Organizational.1235, 1670.12d2Organizational.1

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC9.1.1

Procedure: Business Continuity Plan Development & Maintenance (See Appendix)

1.2 Planning Contents

Business continuity planning must include identification and agreement on all responsibilities, business continuity processes, and the acceptable loss of information and services.

HITRUST 1607.12c2Organizational.4

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)

SOC2 CC7.5.6

1.3 Plan Roles and Responsibilities

The business continuity plan must define the roles and responsibilities for all individuals involved in executing each component of the plan.

HITRUST 1666.12d1Organizational.1235, 1672.12d2Organizational.3

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC5.1.1, CC9.1.1

1.4 Plan Ownership

The business continuity plan must have a formally appointed owner that is responsible for reviewing and updating the plan on at least an annual basis or whenever material changes occur.

HITRUST 1666.12d1Organizational.1235

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC5.1.1, CC9.1.1

1.5 Plan Distribution

Copies of the business continuity plans must be distributed to key contingency personnel.

HITRUST 16.12cNIST80053Organizational.7

HIPAA 164.308(a)(7)(ii)(C)

SOC2 CC7.5.6

1.6 Plan Storage

Business continuity plans must be stored in a remote location.

HIPAA 164.308(a)(7)(ii)(C)

1.7 Plan Security Requirements

The business continuity plan must address a specific, minimal set of relevant information security requirements.

HITRUST 1669.12d1Organizational.8, 1672.12d2Organizational.3

HIPAA 164.308(a)(7)(ii)(C), 164.312(a)(2)(i)

SOC2 CC9.1.1, CC2.1.3

1.8 Critical Business Processes

All critical business processes requiring business continuity must be identified.

HITRUST 1634.12b1Organizational.1

HIPAA 164.308(a)(7)(ii)(B)

SOC2 A1.3.1, CC5.1.3

Procedure: Risk Assessment & Business Impact Analysis (BIA) (See Appendix)

1.9 Identifying Events

Information security aspects of business continuity must be based on identifying events that can cause interruptions to critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters, acts of terrorism).

HITRUST 1635.12b1Organizational.2

HIPAA 164.308(a)(7)(i)

SOC2 A1.3.1, CC7.3.2, CC7.3.3

1.10 Risk Assessments

Business continuity risk assessments must be performed on at least an annual basis with full involvement from owners of business resources and processes. The scope of the assessments must consider all business processes requiring business continuity and identify, quantify, and prioritize risks against key business objectives and criteria, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

HITRUST 1638.12b2Organizational.345

HIPAA 164.308(a)(7)(ii)(E)

SOC2 CC3.2.1, CC3.2.3, A1.2.1

1.11 Risk Assessment Results

Risk assessments must be performed to determine the likelihood and impact of business interruptions, in terms of time, damage scales, and recovery period. The results of the risk assessment must be used to develop a business continuity strategy that identifies the overall approach to business continuity. The strategy must be approved by management and implemented.

HITRUST 1635.12b1Organizational.2

HIPAA 164.308(a)(7)(ii)(E)

SOC2 CC3.2.1, CC3.2.5

NIST CSF id.ra-5, id.ra-6, id.rm-1

1.12 Integrated Security

All identified critical business processes must be integrated with information security management requirements of business continuity and other continuity requirements relating to such aspects as operations, staffing, materials, transports, and facilities.

HITRUST 1636.12b2Organizational.1

HIPAA 164.308(a)(7)(ii)(E)

SOC2 A1.3.1

1.13 Business Impact Analysis

A business impact analysis must be performed on at least an annual basis and used to evaluate the potential consequences of disasters, security failures, loss of service, and service availability.

The goal of the BIA is to illustrate the potential negative impacts due to degraded performance or disruption of the components that make up the business. With this understanding, the business can more effectively allocate resources (for preventive measures and redundancies), select service providers, and prioritize recovery operations.

The BIA report shall document the potential impacts resulting from disruption of business functions and processes. Scenarios resulting in significant business interruption should be assessed in terms of financial impact, if possible.

Through BIA interviews and surveys, business process information shall be collected which includes:

- Name of the process
- Where the process is performed
- Inputs and outputs in the process
- Resources and tools used in the process

- Any process interdependencies
- Impact of a process disruption (financial, operational, regulatory, etc.)
- How the timing and duration of a given disruption affects its impact

After this information is collected, a list of critical processes and a recovery plan should be identified. The BIA should be regularly revisited and updated as new processes are implemented.

HIPAA 164.308(a)(7)(ii)(E)

SOC2 CC3.3.2, CC3.3.3, CC3.3.4

NIST CSF de.ae-4

1.14 System Changes

Business continuity matters must be addressed timely when identified during the management of system changes.

HITRUST 1671.12d2Organizational.2

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC9.1.1, CC8.1.11

1.15 Temporary Operational Procedures

Temporary operational procedures to follow, pending completion of recovery and restoration, must be formally documented and included in the business continuity plan.

HITRUST 1672.12d2Organizational.3

HIPAA 164.308(a)(7)(ii)(C)

SOC2 CC9.1.1

1.16 Contingency Program

A contingency program must be formally documented that addresses capacity requirements, defines critical missions, business functions, recovery objectives and priorities, and identifies roles and responsibilities.

HITRUST 1602.12c1Organizational.4567

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C)

SOC2 CC9.1.1, A1.1.1, A1.1.2, A1.1.3, CC1.4.4

Procedure: Alternate Site & Continuity Infrastructure (See Appendix)

1.17 Alternative Site Agreements

Third-party service agreements must be established with alternative storage and processing sites to allow for the resumption of information systems operations of critical business functions within the time period defined based on a risk assessment, including recovery time objectives.

HITRUST 1604.12c2Organizational.16789

HIPAA 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.310(a)(2)(ii)

SOC2 A1.2.10

1.18 Alternate Site Distances

Alternative storage and processing sites must be physically located at a sufficient distance away from the primary facility and configured with security measures equivalent to the primary site.

HITRUST 1604.12c2Organizational.16789

HIPAA 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 A1.2.10

1.19 Emergency Power and Telecommunications

Emergency power and backup telecommunications must be available at the main site.

HITRUST 1605.12c2Organizational.2

HIPAA 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 A1.2.5

1.20 Alternate Telecommunications

Alternate telecommunications services must be stablished with priority-of-service provisions and sufficiently separated from the primary service provider.

HITRUST 1609.12c3Organizational.12

HIPAA 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 A1.2.5

1.21 Emergency and Fallback Procedures

Business process owners must formally document and maintain emergency procedures, manual fallback procedures, and resumption plans for their areas.

HITRUST 1668.12d2Organizational.5

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC5.1.1

NIST CSF pr.pt-5, id.be-5, pr.ip-9

1.22 Service Provider Fallback Arrangements

Service providers must formally document and maintain fallback arrangements for all alternative technical services, such as information processing and communications facilities.

HITRUST 1668.12d2Organizational.5

HIPAA 164.308(a)(7)(ii)(C), 164.310(a)(2)(i)

SOC2 CC5.1.1

NIST CSF pr.pt-5, id.sc-3, id.sc-5

1.23 New Requirements

When new requirements are identified, emergency procedures, manual fallback procedures, and resumption plans must be amended as appropriate.

HITRUST 1667.12d2Organizational.4

HIPAA 164.308(a)(7)(ii)(C)

SOC2 CC5.1.1

NIST CSF rc.im-2

2.0 Disaster Recovery

2.1 Restoration

Business operations and availability of information must be restored successfully in the time frame required by business objectives, without a deterioration of the security measures.

HITRUST 1601.12c2Organizational.7

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(B), 164.310(a)(2)(i)

SOC2 A1.2.9, A1.2.10

NIST CSF rc.rp-1

Procedure: Disaster Recovery & Restoration (See Appendix)

2.2 Backups

Backups of information and software must be made and tests of the media and restoration procedures must be regularly performed at appropriate intervals.

HITRUST 1616.09l1Organizational.16

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E)

SOC2 A1.2.7, A1.2.8, A1.2.9, A1.3.2

NIST CSF pr.ip-4, id.sc-5, pr.ip-10

Procedure: Backup Procedure (See Appendix)

2.3 Backup Definitions

Formal definitions of the level of backup required for each critical system must be defined and documented and at a minimum, include the following elements:

- Restoration procedures for each system
- Scope of the data to be backed up

- Backup frequency
- Retention period based on relevant contractual, legal, regulatory, business requirements.

HITRUST 1617.09l1Organizational.23

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(B)

SOC2 A1.2.7, A1.2.8, A1.2.9

NIST CSF id.be-5, rc.co-3

2.4 Backup Schedule

Incremental or differential backups must be performed on a daily basis, and full backups must be performed on a weekly basis to separate media.

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E)

SOC2 A1.2.8

2.5 Sensitive Data

Sensitive data must be backed up in an encrypted format to ensure confidentiality.

HITRUST 1623.09l2Organizational.4

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E)

SOC2 CC6.1.9

NIST CSF pr.ip-4

2.6 Automated Tools

Automated tools must be utilized to track all backups.

HITRUST 1621.09l2Organizational.1

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(A), 164.312(c)(1)

SOC2 A1.2.8

2.7 Backup Testing

Backups must be tested following the initial completion of each backup type for reliability and integrity. All backups must additionally best tested on at least an annual basis after the initial test.

HITRUST 1627.09l3Organizational.6

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E), 164.312(c)(1), 164.308(a)(7)(ii)(D)

SOC2 A1.3.2

NIST CSF pr.ip-4

2.8 BYOD Backup Roles

Bring Your Own Device (BYOD) data backup roles and responsibilities for workforce members must be clearly identified and communicated. In particular, users must be required to perform backups of organizational and/or client data on their BYOD devices.

HITRUST 1699.09l2Organizational.6

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(A)

SOC2 A1.2.7

NIST CSF pr.ip-9, pr.ip-4

2.9 Third-Party Backup Services

When backup services are delivered by a third-party, a service level agreement must be formally documented and executed that includes detailed protections to control confidentiality, integrity, and availability of the backup information.

HITRUST 1620.09l1Organizational.8

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E), 164.312(c)(1)

SOC2 CC9.2.1

NIST CSF id.sc-3, id.sc-4

2.10 Backup Storage

Backups must be stored in a physically secure remote location that is a sufficient distance away from the primary site to make them reasonably immune from damage to the primary site. Reasonable physical and environmental controls must be in place to ensure protection of the backups at the remote location.

HITRUST 1618.09l1Organizational.45

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E), 164.312(c)(1)

SOC2 A1.2.9

2.11 Backup Copies

Backup copies must be maintained to ensure integrity, security, and future availability. Any potential accessibility problems with backup copies must be identified and mitigated promptly in the event of an area-wide disaster.

HITRUST 1622.09l2Organizational.23

HIPAA 164.308(a)(7)(ii)(E), 164.312(c)(1)

SOC2 A1.2.9, A1.3.2

NIST CSF pr.ip-4, id.be-5

2.12 Backup Retention

At least three generations of backups (full, incremental, and differential) must be stored offsite.

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E)

SOC2 A1.2.9

2.13 Server Movement

A current and retrievable copy of critical data must be made available before the movement of servers on which the data resides.

HITRUST 1626.09l3Organizational.5

HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.310(d)(2)(iv)

SOC2 A1.2.7

2.14 Backup Storage Logging

Backups stored onsite and offsite must be logged and include backup name, date, time, and action.

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E)

SOC2 A1.2.6

NIST CSF pr.ip-4

2.15 Inventory Records

Inventory records must be maintained for backup copies, which include content description and current location.

HITRUST 1619.09l1Organizational.7

HIPAA 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(E), 164.312(c)(1)

SOC2 A1.2.9

NIST CSF id.am-5

Procedures Appendix

Alternate Site & Continuity Infrastructure

Purpose: Ensure infrastructure and third-party arrangements exist to sustain operations during a disruption.

Procedure:

1. Document a formal contingency program covering capacity requirements, critical missions/functions, recovery objectives/priorities, and roles/responsibilities.
2. Establish third-party agreements with alternate storage/processing sites sufficient to resume critical operations within the recovery time objective (RTO) defined by the risk assessment.
3. Confirm alternate sites are physically distant enough from the primary facility to avoid shared-disaster risk, and configured with security controls equivalent to the primary site.
4. Maintain emergency power and backup telecommunications at the main site.
5. Establish alternate telecommunications service with priority-of-service provisions, using a provider sufficiently separated from the primary provider.
6. Business process owners document and maintain emergency procedures, manual fallback procedures, and resumption plans for their areas.
7. Service providers document and maintain their own fallback arrangements for alternative technical services (processing, communications).
8. When new requirements are identified (new systems, new risks, audit findings), amend emergency/fallback/resumption plans accordingly and re-distribute.

Responsible party: BC Plan Owner (contingency program); Procurement/Vendor Management (site & telecom agreements); Business process owners (emergency/fallback docs); IT/Facilities (power & telecom).

Backup Procedure

Purpose: Ensure critical data and systems are reliably backed up, protected, tested, and recoverable.

Procedure:

1. Define and document backup requirements for each critical system, including: restoration procedure, scope of data backed up, backup frequency, and retention period (per contractual/legal/regulatory/business requirements).
2. Perform incremental or differential backups daily; perform full backups weekly to separate media.
3. Encrypt all backups containing sensitive data.
4. Use automated tools to track all backup jobs (success/failure, timing, scope).
5. Test each backup type immediately after its initial run for reliability and integrity; retest at least annually thereafter.
6. Store backups at a physically secure, remote location sufficiently distant from the primary site to survive a site-wide event; apply physical/environmental controls at that location.
7. Retain at least three generations of backups (full, incremental, differential) offsite.
8. Before moving any server, create and verify a current, retrievable copy of the critical data it holds.
9. Log every backup stored onsite or offsite: name, date, time, and action taken.
10. Maintain an inventory record for all backup copies, including content description and current location.

11. If backup accessibility issues are identified (e.g., during an area-wide event), document and mitigate promptly.

Responsible party: IT Operations (execution, testing, logging); Data/System Owners (backup definitions); IT Security (encryption compliance).

Business Continuity Plan Development & Maintenance

Purpose: Ensure a formal, maintained, and properly protected BC plan exists for every business unit.

Procedure:

1. Each business unit documents a formal business continuity plan covering: minimum approach to maintain information/asset availability and security, an escalation plan, and activation conditions.
2. Plan includes agreed responsibilities, continuity processes, and acceptable loss thresholds for information and services.
3. Plan explicitly assigns roles and responsibilities for every individual involved in executing each plan component.
4. A formally appointed plan owner is assigned per business unit; owner reviews and updates the plan at least annually or upon material change.
5. Owner distributes current copies of the plan to all key contingency personnel.
6. A copy of the plan is stored at a remote (off-primary-site) location.
7. Plan owner ensures the plan addresses the minimal relevant information security requirements (access control, data protection during activation, etc.).
8. Plan owner logs each review/update with date, version, and summary of changes.

Responsible party: Business unit leadership (content); designated Plan Owner (review, distribution, storage).

Disaster Recovery & Restoration

Purpose: Ensure business operations and data availability are restored within required timeframes without weakening security.

Procedure:

1. Upon disruption, activate the relevant BC plan's escalation and recovery process.
2. Restore business operations and information availability within the timeframe required by business objectives (per defined RTOs), ensuring no reduction in security controls during restoration.
3. For BYOD devices, workforce members follow their assigned backup responsibilities (communicated in advance) and perform required backups of organizational/client data on those devices.
4. Where backup services are provided by a third party, confirm a signed SLA is in place covering confidentiality, integrity, and availability protections for backup data before relying on that provider during recovery.
5. Document the recovery timeline, actions taken, and any deviations from plan for post-incident review.
6. Conduct a post-recovery review to identify gaps and feed lessons learned back into the BC plan and BIA.

Responsible party: IT Operations/Disaster Recovery team (execution); BC Plan Owner (escalation, post-incident review); Employees with BYOD (individual backup compliance).

Risk Assessment & Business Impact Analysis (BIA)

Purpose: Identify critical business processes and quantify the impact of potential disruptions to drive recovery priorities.

Procedure:

1. Identify and document all critical business processes requiring business continuity coverage.
2. Identify events that could interrupt those processes (equipment failure, human error, theft, fire, natural disaster, terrorism, etc.).
3. Conduct a business continuity risk assessment at least annually, with full involvement of resource/process owners; assess critical resources, disruption impacts, allowable outage times, and recovery priorities.
4. Use risk assessment results to quantify likelihood/impact (time, damage scale, recovery period) and develop a BC strategy; obtain management approval before implementation.
5. Integrate identified critical processes with security, staffing, materials, transport, and facilities continuity requirements.
6. Conduct a Business Impact Analysis (BIA) at least annually:
    - Interview/survey process owners to capture: process name, location, inputs/outputs, resources/tools used, interdependencies, disruption impact (financial/operational/regulatory), and timing/duration sensitivity.
    - Document potential financial impact of significant disruption scenarios.
    - Produce a prioritized list of critical processes and associated recovery plan.
7. Revisit and update the BIA whenever new processes are implemented.
8. Address business continuity implications during any system change management process, in a timely manner.

Responsible party: Business process owners (input); BC Plan Owner (assessment coordination); Management (strategy approval).

Release and Review History

Action	User	Date
Released Version 1.0	Amanda Ates Manager	07/06/2026, 4:45:00 PM