Business Continuity Policy

ACME Evil Anvil Corporation

March 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to ensure that the organization establishes objectives, plans and, procedures such that a major disruption to the organization's key business activities is minimized.

b. This policy applies to all infrastructure and data within the organization's information security program.

c. This policy applies to all management, employees, and suppliers that are involved in decisions and processes affecting the organization's business continuity. This policy must be made readily available to all whom it applies to.

2 Background

a. The success of the organization is reliant upon the preservation of critical business operations and essential functions used to deliver key products and services. The purpose of this policy is to define the criteria for continuing business operations for the organization in the event of a disruption. Specifically, this document defines:

   i. The structure and authority to ensure business resilience of key processes and systems.

   ii. The requirements for efforts to manage through a disaster or other disruptive event when the need arises.

   iii. The criteria to efficiently and effectively resume normal business operations after a disruption.

b. Within this document, the following definitions apply:

   i. *Business impact analysis/assessment* - an exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to return to a normal level of operation, and prioritizes recovery of processes and the supporting system.

   ii. *Disaster recovery plan* - a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, when an activity is interrupted by an emergency or disaster.

   iii. *Recovery time objective* - the amount of time allowed for the recovery of a business function or resource to a normal level after a disaster or disruption occurs.

iv. *Recovery point objective* - determined based on the acceptable data loss in the case of disruption of operations.

3 Policy

a. *Business Risk Assessment and Business Impact Analysis*

i. Each manager is required to perform a business risk assessment and business impact analysis for each key business system within their area of responsibility.

ii. The business risk assessment must identify and define the criticality of key business systems and the repositories that contain the relevant and necessary data for the key business system.

iii. The business risk assessment must define and document the Disaster Recovery Plan (DRP) for their area of responsibility. Each DRP shall include:

1. Key business processes.
2. Applicable risk to availability.
3. Prioritization of recovery.
4. Recovery Time Objectives (RTOs).
5. Recovery Point Objectives (RPOs).

b. *Disaster Recovery Plan*

i. Each key business system must have a documented DRP to provide guidance when hardware, software, or networks become critically dysfunctional or cease to function (short and long term outages).

ii. Each DRP must include an explanation of the magnitude of information or system unavailability in the event of an outage and the process that would be implemented to continue business operations during the outage. Where feasible, the DRP must consider the use of alternative, off-site computer operations (cold, warm, hot sites).

iii. Each plan must be reviewed against the organization's strategy, objectives, culture, and ethics, as well as policy, legal, statutory and regulatory requirements.

iv. Each DRP must include:

1. An emergency mode operations plan for continuing operations in the event of temporary hardware, software, or network outages.

2. A recovery plan for returning business functions and services to normal on-site operations.
3. Procedures for periodic testing, review, and revisions of the DRP for all affected business systems, as a group and/or individually.

c. *Data Backup and Restoration Plans*

i. Each system owner must implement a data backup and restoration plan.

ii. Each data backup and restoration plan must identify:

1. The data custodian for the system.
2. The backup schedule of each system.
3. Where backup media is to be stored and secured, as well as how access is maintained.
4. Who may remove backup media and transfer it to storage.
5. Appropriate restoration procedures to restore key business system data from backup media to the system.
6. The restoration testing plan and frequency of testing to confirm the effectiveness of the plan.
7. The method for restoring encrypted backup media.