12.2.4 Business Continuity Facts

Business continuity is the ability to provide critical business functions for customers, suppliers, regulators, and other entities. Business continuity activities are performed daily to maintain service, consistency, and recoverability.

Business Continuity Documents

The following table explains the organizational plans and documents business continuity requires.

Plan Type	Description
Business Continuity Plan (BCP)	A BCP identifies appropriate disaster responses that allow business operations to continue when infrastructure and resource capabilities are restricted or reduced. This ensures that critical business functions (CBF) can be performed when operations are disrupted. Additionally, a BCP identifies the actions required to restore the business to normal operation. A BCP: ▪ Identifies and prioritizes critical functions. ▪ Calculates recovery timeframes. ▪ Contains plans, including resource dependencies and response options, to bring critical functions online within an established timeframe. ▪ Specifies procedures for securing unharmed assets and salvaging damaged assets. ▪ Identifies BCP team members who are responsible for plan implementation. ▪ Should be tested on a regular basis to verify that the plan still meets recovery objectives.
Business Impact Analysis (BIA)	A BIA focuses on the impact that losses will have on the organization. A BIA: ▪ Identifies threats that can affect processes and assets. ▪ Establishes the maximum down time (MDT) the corporation can survive without each process and asset. ▪ Estimates tangible impacts (such as financial loss) and intangible impacts (such as loss of customer trust) on the organization.
Disaster Recovery Plan (DRP)	A DRP identifies short-term actions that can stop the incident and restore critical functions so the organization can continue to operate. The DRP is a subset of the BCP. The DRP is the plan for IT-related recovery and continuity. A DRP should include: ▪ Guidelines for restoring applications, data, hardware, communications, and other IT infrastructure in case of disaster. ▪ Consideration of every possible failure. ▪ Plans for converting operations to alternative sites in case of disaster. ▪ Plans for converting back to the original site after the disaster has concluded. ▪ Disaster recovery exercises (such as fire drills) that simulate a possible disaster.

How to Create a DRP and BCP

The following list contains best practices for creating a DRP and BCP.

- Document all important decisions before the disaster strikes. When a disaster occurs, staff members simply need to follow the documented procedures.
- Divide disaster response into phases.
    1. Identify the disaster, ensure the safety of personnel, and begin recovery procedures.
    2. Implement short-term recovery mechanisms to bring the most critical business systems online (also known as mission-critical systems).
    3. Stabilize operations by restoring supporting departments and functions.
    4. Carry out measures to restore all functions to normal. Switch from temporary procedures back to normal operating procedures.
- Define team member roles and responsibilities. This will ensure a separation of roles and a clear chain of command.
- Define the testing and training of team members. Team members should include representatives from all major parts of the corporation.
- Conduct regular practices and training exercises to test portions of the plan. Revise the plan and training as necessary.
- As a BCP or DRP evolves over time, it is essential to collect and destroy all outdated copies of the plan as a new version is rolled out.
- Assign responsibility for ongoing maintenance of the BCP and DRP.