# 3.3.2 Business Continuity Facts

*Business continuity* is the activity performed by an organization to ensure that critical business functions are available to customers, suppliers, regulators, and other entities that must have access to those functions. Business continuity:

- Refers to activities performed daily to maintain service, consistency, and recoverability.
- Is not something implemented at the time of a disaster.

Be aware of the following plans pertaining to business continuity:

| Plan Type | Description |
|---|---|
| Business Continuity Plan (BCP) | The Business Continuity Plan (BCP) identifies appropriate disaster responses that maintain business operations during reduced or restricted infrastructure and resource capabilities. In addition, a BCP identifies actions required to restore the business to normal operation. A business continuity plan is designed to ensure that critical business functions (CBF) can be performed when operations are disrupted. Development of a BCP manual to document and track progress of the BCP would include the following steps:<br>1. Analysis<br>2. Solution design<br>3. Implementation<br>4. Testing and organization acceptance<br>5. Maintenance<br><br>A BCP:<br>- Identifies and prioritizes critical functions.<br>- Calculates recovery timeframes.<br>- Identifies plans, including resource dependencies and response options, to bring critical functions online within an established timeframe. These plans spell out a clear order of restoration based on company needs and priorities, as well as legal responsibilities to customers and shareholders.<br>- Specifies procedures for security of unharmed assets.<br>- Identifies procedures for salvage of damaged assets.<br>- Identifies BCP team members who are responsible for plan implementation.<br>- Should be tested on a regular basis to verify that the plan still meets recovery objectives. Three different types of tests are commonly used:<br>  - In a *tabletop exercise*, a small number of individuals get together and test just one part of the BCP. They typically work through a simple scenario and then analyze the plan to identify any changes that may be necessary.<br>  - In a *medium exercise*, a larger number of individuals get together and work though a larger-scale simulation that incorporates many parts of the BCP. Medium exercises incorporate a higher degree of realism than a tabletop exercise. Once complete, the participants analyze the plan to identify any changes that may be necessary.<br>  - A *complex exercise* involves a very large number of individuals and a very realistic scenario that may involve full-scale practice exercises.<br><br>Continuity of Operations Planning (COOP) is similar to a BCP, but can also refer to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. |
| Business Impact Analysis (BIA) | A Business Impact Analysis (BIA) focuses on the impact losses will have on the organization. A BIA:<br>- Identifies threats that can affect processes/assets.<br>- Identifies mission-essential functions.<br>- Identifies critical systems.<br>- Establishes the maximum down time (MDT) the corporation can survive without the process/asset.<br>- Establishes other recovery benchmark values.<br>  - Recovery Point Objective (RPO)<br>  - Recovery Time Objective (RTO)<br>  - Mean time between failures (MTBF)<br>  - Mean time to repair (MTTR)<br>- Estimates tangible (financial loss) and intangible (e.g., loss of customer trust) impact on the organization.<br>  - Life<br>  - Property<br>  - Safety<br>  - Finance<br>  - Reputation<br><br>Senior management may mistakenly view the security program as a cash drain rather than a cost-saving implementation. The BIA should be used to demonstrate the cost savings of the security program. |

| | |
|---|---|
| Disaster Recovery Plan (DRP) | The Disaster Recovery Plan (DRP) identifies short-term actions necessary to stop the incident and restore critical functions so the organization can continue to operate. The DRP is a subset of the BCP, and is the plan for IT-related recovery and continuity. A disaster recovery plan (DRP) should include:<br>▪ Plans for resumption of applications, data, hardware, communications, and other IT infrastructure in case of disaster.<br>▪ Attempts to take into consideration every failure possible.<br>▪ Plans for converting operations to alternate processing sites in case of disaster.<br>▪ Plans for converting back to the original site after the disaster has concluded.<br>▪ Disaster recovery exercises (such as fire drills) that simulate a possible disaster.<br><br>Decisions about alternate site locations need to be guided by the following requirements:<br>▪ Maintain adequate geographic distance between primary and secondary sites. Such geographic diversity can minimize the possibility of a disaster bringing down both sites.<br>▪ Site locations can have legal implications, especially when data is stored in multiple countries. *Data sovereignty* refers to the fact that every country has its own laws and regulations regarding digital data storage. Data safety and privacy concerns may need to be reassessed for each location.<br>▪ Decide whether the backup site will be hot or cold. A hot site is set up with servers and workstations that have almost immediate access to data that is continuously replicated from the main site. If this is too expensive, a cold site, such as an empty warehouse, can be used. The disadvantage of a cold site is that it will take much longer to install the necessary hardware and software necessary to resume business operations.<br>▪ Whether a hot or a cold site is chosen as a backup, alternate business practices and processes need to be defined and stored in each location. Critical tasks should be described in sufficient detail to allow business staff to carry them out with minimal training. |

Keep in mind the following when creating the disaster recovery and business continuity plans:

- A good plan documents all important decisions before the disaster strikes. When a disaster occurs, staff members simply need to follow the documented procedures.
- Disaster response is typically divided into phases:
  1. Identify the disaster, ensure safety of personnel, and begin to implement recovery procedures.
  2. Implement short-term recovery mechanisms to bring mission-critical systems online.
  3. Stabilize operations by restoring supporting departments and functions.
  4. Implement measures to restore all functions to normal. Switch back from temporary measures to normal operating procedures. The order of restoration is defined in the BCP and then carried out in this last phase. A typical restoration order begins with the systems, databases, and applications that are most critical to the continued operation of the business. The order of restoration will often vary significantly from one company to another.
- Define processes for implementing, testing, and training team members. Team members should be representatives from all major parts of the corporation.
- After the plan has been created, conduct regular practices and training exercises to test portions of the plan. Revise the plan or training as necessary.
- As a BCP or DRP plan evolves over time, it is essential to collect and destroy all outdated copies of the plan as a new version of a plan is rolled out.
- Assign responsibility for ongoing maintenance of the BCP and DRP plans.

*Succession planning* is a process for identifying and developing internal people with the potential to fill key positions at some point in the future within an organization. Succession planning:

- Increases the availability of experienced and capable employees that are prepared to assume specific roles as they become available.
- Ensures that the right competencies are recruited into the organization, nurtured and developed over time to guarantee smooth transitions for future vacancies.
- Contrasts *replacement planning*, which focuses on identifying specific backup candidates for given positions.

---