



Excerpts from...

Business Continuity and Disaster Recovery Solutions

...being prepared and responding during a crisis

December 16, 2020 / Fred Hencke

© 2020 by The Segal Group, Inc.



Business Continuity and Disaster Recovery

Business Continuity (BC) and Disaster Recovery (DR) are closely related practices that support an organization's ability to remain operational after an adverse event.



Business Continuity Plan (BCP)

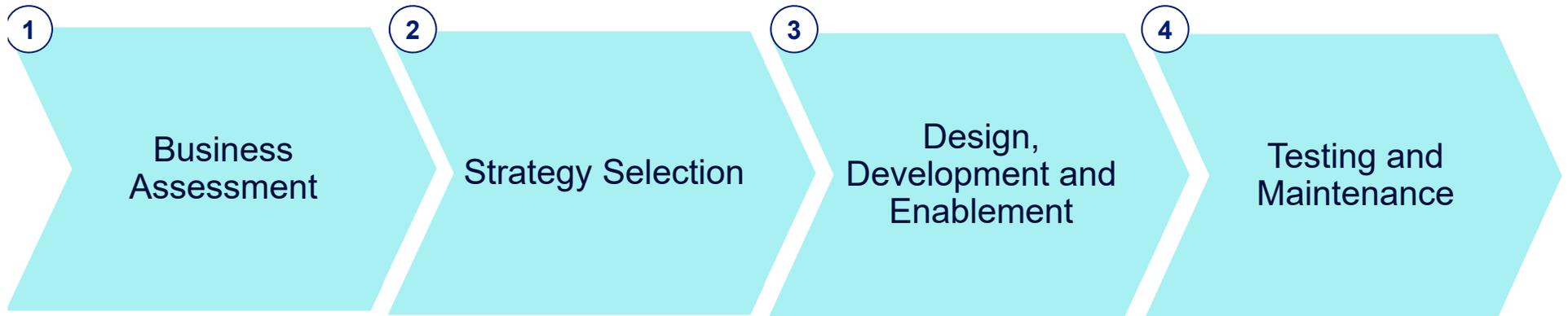
A comprehensive plan with an integrated set of procedures and up-to-date resource information used to guide the **recovery** from a disaster causing major disruption to business operations.

Said another way...

It is intended to minimize the effects of outages and disruptions on business operations, enabling an organization to get back to operating after a problem occurs while reducing risks to employees, customers, suppliers, reputation and potential data loss.



BCP Development - approach



Senior management alignment

Risk assessment (for each relevant disaster)

Impact Analysis

Points of failure

Recovery time objectives (RTO)

Minimum resource requirements

Emergency management team (EMT)

Recovery team

RTO viability

Update rosters and action plans

Senior management alignment

Facilitate alignment and approval for the following:

- The disaster types to include in scope
- Stakeholders and resources to include on the BCP development team
- Budget approval (to develop the BCP initially; may need additional approvals to better equip and enable emergency management and recovery teams should a disaster occur)



Business assessment objectives (risk assessment)

Identify external and internal threats to the business, and:

- critical processes (and flow) and resources in each business unit / functional area
- recovery time objectives for each critical process
- existing and potential disaster – mitigating systems and procedures
- existing containment measures and exposures



Business assessment objectives (impact analysis)

What does a Business Impact Analysis (BIA) provide to the organization?

- an independent view of risks from a disaster situation
- a basis for determining cost-effective strategies
- identification of critical and necessary business functions/processes and their resource dependencies
- identification of critical computer systems and their associated outage tolerance
- estimates of the financial and operational impacts resulting from the disruption and the required recovery time frames for the critical business functions (Recovery Time Objectives – RTO)
- business case for strategy selection



Strategy selection objectives

To define the actions needed to protect the organization and to select the most appropriate recovery solutions for critical business functions and supporting resources.

- address single points of failure
- balance business impact with cost to recover
- develop alternatives to define and refine minimum resource requirements for recovery, including the following considerations:
 - computer and network operations
 - voice and data communications
 - work area requirements (space, equipment, supplies, vital records, etc.)
 - staffing levels
 - geography and transportation
 - business unit independence



Testing and maintenance objectives

Once the BCP has been completed and approved by senior management, it must now be tested and maintained.

- Testing – determines if documented recovery strategies and procedures are viable to recover critical business functions within their stated RTO
- Maintenance – Within a year or less, the BCP becomes much less useful because staff and vendors have changed, and resources needed to serve customers have evolved. Periodically, throughout the year, re-examine and update action plans and supporting documents (e.g., location information, computer system schematics, etc.)



Mistakes to avoid

Avoid the following common mistakes:

- Lack of Senior management engagement and support
- Failure to comply with applicable standards
- Not performing a risk and business impact analysis
- Failure to define strategies for response, recovery, restoration and resumption of business activities
- Not defining incident response and damage assessment activities
- Not testing the BCP
- Not maintaining the BCP

