

# **CIT 270: SYSTEMS SECURITY I**

## **CHAPTER 14: BUSINESS CONTINUITY**

# INTRODUCTION

---

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note 

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to **yellow words**. These highlighted words denote a topic that will almost always be on your chapter quiz.



# WHAT IS BUSINESS CONTINUITY?

---

**Business continuity** planning (BCP) is defined as the ability of an organization to maintain its operations and services in the face of a disruptive event and consists of three essential elements:

1. Business recovery planning.
2. Crisis management and communications.
3. Disaster recovery.

# WHAT IS BUSINESS CONTINUITY?

---

<u>Terminology</u>	<u>Description</u>	<u>How this compares to BCP</u>
Resumption Planning	Used for recovery of critical business functions from IT, such as resuming a critical manufacturing process	Part of the BCP process.
Contingency Actions	Tactical solutions addressing a core business resource or process, such as how to handle the loss of a specific vendor	Contingency planning is usually considered an isolated action and not a part of an overall BCP
Emergency Response	The immediate actions taken to preserve lives and safeguard property and assets, such as an evacuation plan	Emergency response is a subset of a BCP
Disaster Recovery	The recovery and resumption of critical technology assets in the event of a disaster	Disaster recovery is a component of an overall BCP program



# WHAT IS BUSINESS CONTINUITY?

---

**Business Impact Analysis (BIA):** identifies business functions and quantifies the impact a loss of these functions may have on business operations.

- **impact on property** (tangible assets)
- **impact on finance** (monetary funding)
- **impact on safety** (physical protection)
- **impact on reputation** (status)
- **impact on life** (wellbeing)

# WHAT IS BUSINESS CONTINUITY?

---

**Mission-essential Function:** the activity that serves as the core purpose of the organization; providing health care for a hospital.

**Critical Systems:** systems or business processes that support the mission-essential function; maintain a working emergency room.

**Single Point of Failure:** a component or entity in a system which, if it no longer functions, will disable the entire system; patient database.

**High Availability:** a system that can function for an extended period of time with very little downtime; see page 611.



# WHAT IS BUSINESS CONTINUITY?

---

**Privacy Impact Assessment:** part of a BIA that is used to identify and mitigate privacy risks.

**Privacy Threshold Assessment:** determines if a system contains personally identifiable information (PII), if a privacy impact assessment is needed, and if any other privacy requirements are needed; updated software, network change.

**Disaster Recovery Plan:** created by the organization to address how restoring IT functions and services to their former state will be handled in the event of a significant disruption in service.

- order of restoration
- alternative business practices (workarounds)
- failover

# FAULT TOLERANCE THROUGH REDUNDANCY

---

**Redundancy:** the use of duplicated equipment to improve system availability.

**Mean Time to Recovery (MTTR):** a variable in a systems redundancy capabilities; a server with dual power supplies has zero MTTR.

**Mean Time Between Failures (MTBF):** a statistical value used to determine the mean (average) of how many spare parts are needed to be kept on hand; when will *these* fail?



# FAULT TOLERANCE THROUGH REDUNDANCY

---

**RAID (Redundant Array of Independent Drives)** uses multiple hard drives for increased reliability and performance.



RAID levels 0, 1, 4, 5,  
6, 10, 50 explained




What is RAID 0, 1, 2, 3,  
4, 5, 6 and 10 (1+0)?

# FAULT TOLERANCE THROUGH REDUNDANCY: RECOVERY SITES

---

Redundancy is not just about having back IT infrastructure or power, it is also about have a plan for complete business redundancy.



 Cold Site, Hot Site, and Warm Site - CompTIA  
Security+ SY0-401: 2.8



# FAULT TOLERANCE THROUGH REDUNDANCY: DATA

---

**Data Backup:** copying information to a different medium and storing it at an off-site location.

**Recovery Point Objective (RPO):** the first element used in calculating when backups should be performed. This is the *age* of the data, the answer to the question *how long can we tolerate between backups?*

**Recovery Time Objective (RTO):** the second element used in calculating when backups should be performed. This is the length of time it would take to recover data that has been backed up.

# FAULT TOLERANCE THROUGH REDUNDANCY: DATA

## Types of data backups:

<u>Type</u>	<u>How its Used</u>	<u>Archive Bit After Backup</u>	<u>Files Needed for Recovery</u>
Full Backup	Starting point of all backups	Cleared (set to 0)	The full backup is needed
Differential Backup	Backs up any data that has changed since the last full backup	Not cleared (set to 1)	The full backup and only last differential backup are needed
Incremental Backup	Backs up any data that has changed since last full backup or last incremental backup	Cleared (set to 0)	The full backup and all incremental backups are needed



# FAULT TOLERANCE THROUGH REDUNDANCY: DATA

---

**Snapshot:** continuous data protection (CDP) that backups data continuously and can be restored immediately. CDP maintains a historical record of all changes made to data by constantly monitoring writes of data.

No matter which methods of redundancy and data protection you use you must also factor in:

- legal implications like data sovereignty
- location
- distance

# ENVIRONMENTAL CONTROLS

---

Read pages 628 – 632.



# Incident Response

---

Read pages 633 – 639.