



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security and Compliance Week 6 : Planning for Contingencies

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsc.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Discuss the need for contingency planning
- Describe the major components of incident response, disaster recovery, and business continuity
- Define the components of an Incident Response model
- Discuss how the organisation would prepare and execute a test of contingency plans

Key Concepts

- Contingency planning models
- Incident Response models
- Business continuity models
- Crisis management methods

Chapter 10: Planning for Contingencies

INTRODUCTION TO CONTINGENCY PLANNING

Introduction

- The Importance of planning for unexpected adverse events that disrupt technology and halt business operations.
- Effective disaster planning and execution are critical to safeguarding an organization's information resources and assets.
- Failure to plan can result in irreparable damage, risking the organization's recovery and continuity.
- Statistic: Over 40% of businesses without a disaster plan close permanently after a major loss (source: Hartford Insurance Company).

Fundamentals of Contingency Planning

- **Contingency Planning (CP):** Overall strategy for addressing unexpected adverse events.
- Aims to prepare for, detect, react to, and recover from threats to information security and assets.

Main Goal: Restore normal operations with minimal cost and disruption to business activities.

NIST CP Methodology

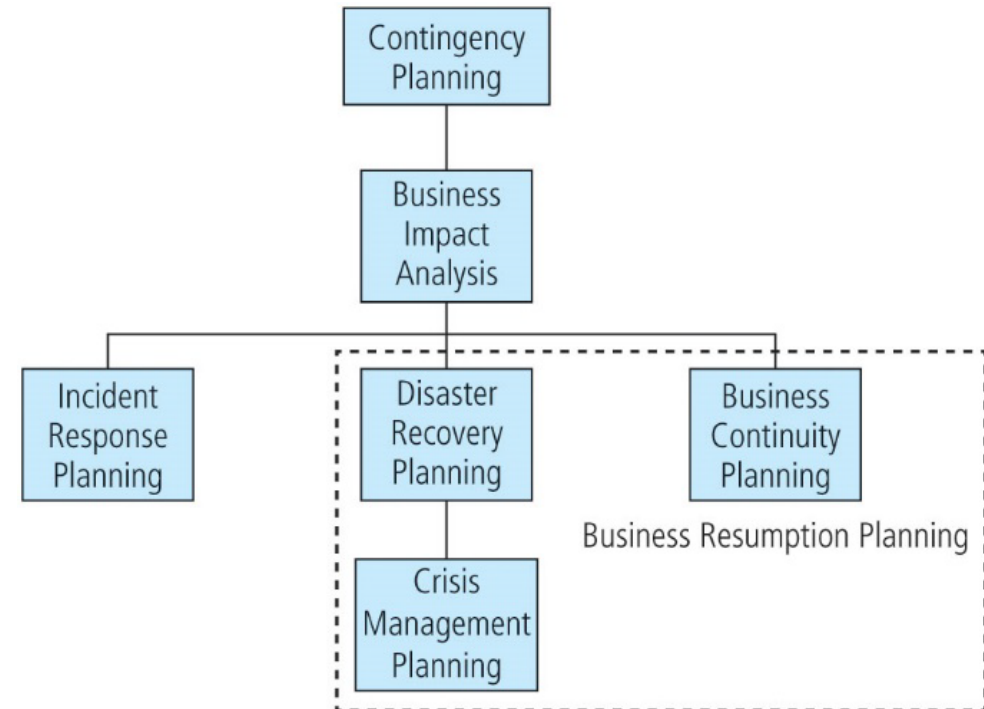
- **Contingency Planning Management Team (CPMT):** Develops the CP document.
- **NIST Recommended Steps:**
 - Develop the CP policy statement.
 - Conduct the Business Impact Analysis (BIA).
 - Identify preventive controls.
 - Create contingency strategies.
 - Develop a contingency plan.
 - Ensure plan testing, training, and exercises.
 - Ensure plan maintenance.

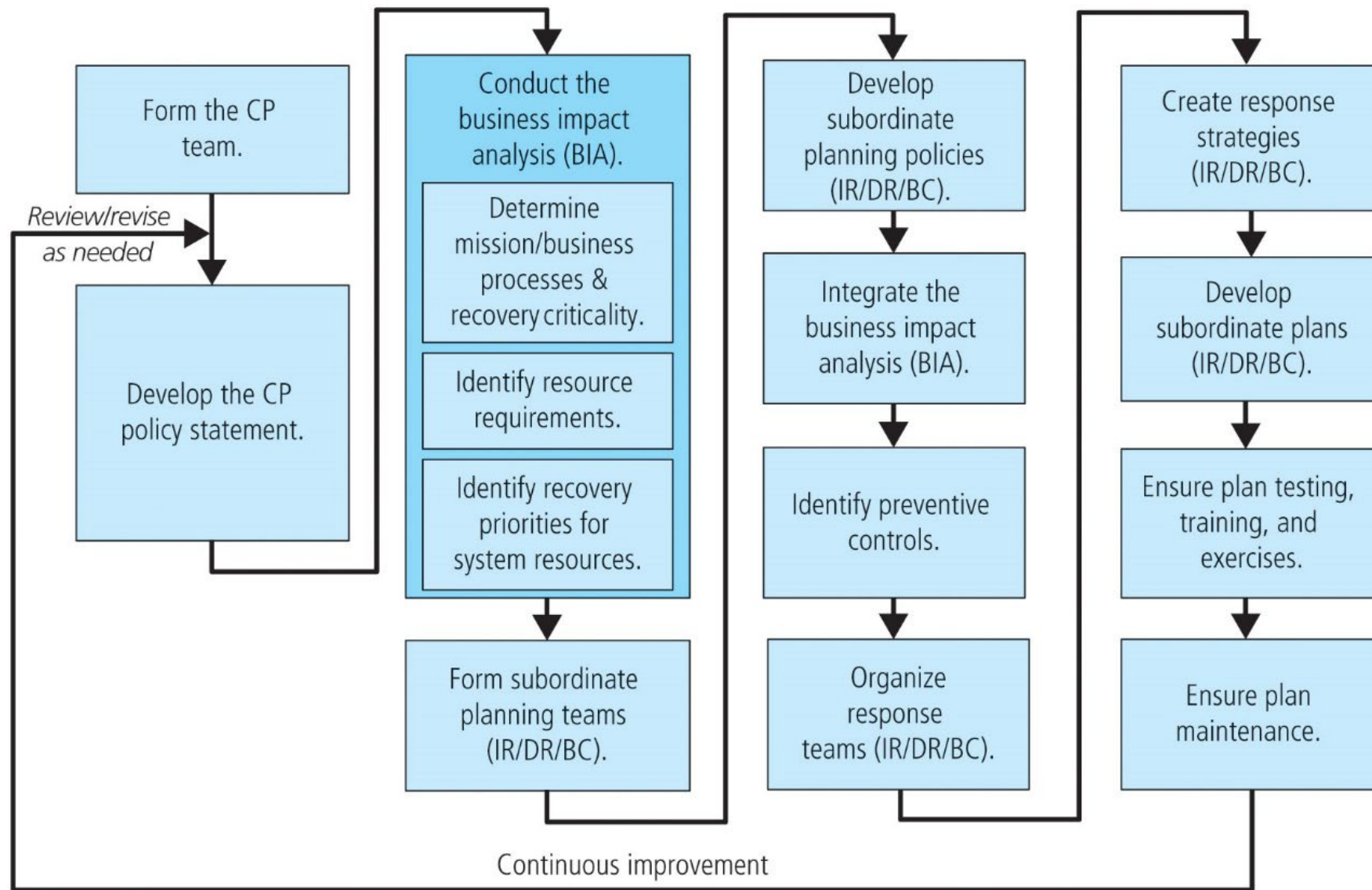
Contingency Planning Policy Components

- An introductory statement by senior management
- The scope and purpose of the CP operations
- A call for periodic risk assessment and BIA by the CPMT
- A description of the major components of the CP
- A call for, and guidance in, the selection of recovery options and business continuity strategies
- A requirement to test the various plans on a regular basis
- Identification of key regulations and standards that impact CP planning and a brief overview of their relevancy
- Identification of key individuals responsible for CP operations
- An appeal for support to the individual members of the organizations
- Additional administrative information

Individuals and Teams involved in CP

- The **Contingency Planning Management Team (CPMT)** including:
 - Champion
 - Project Manager
 - Team Members
 - Business managers
 - Information technology managers
 - Information security managers
 - Representatives of the supplemental teams (IR, DR, BC)
- In addition to the Contingency planning teams:
 - IR Team
 - DR Team
 - BC Team





CP Components

- CP consists of four major components:
 1. Business impact analysis (BIA)
 2. Incident response plan (IR plan)
 3. Disaster recovery plan (DR plan)
 4. Business continuity plan (BC plan)
- Depending on the organisation's size and business philosophy, IT and InfoSec managers can either
 - Can be developed as one unified plan.
 - Created separately with interlocking procedures to ensure continuity.

Business Impact Analysis (BIA)

- **Business Impact Analysis (BIA):** The first phase of the Contingency Planning (CP) process.
- **Purpose:** Investigates and assesses the impact of adverse events on the organisation.
- **Key Difference from Risk Management:**
 - Risk management identifies threats, vulnerabilities, and controls to protect information.
 - BIA assumes that controls have failed, the attack succeeded, and adversity has occurred.

Business Impact Analysis (BIA) process

- **Business Impact Analysis (BIA):**
 - Begins with the prioritised list of threats and vulnerabilities from the risk management process.
 - Enhances the list with additional information for effective adversity response.
- **Key Considerations in BIA:**
 - **Scope:** Define the boundaries of the analysis.
 - **Plan:** Establish a structured approach.
 - **Balance:** Ensure resource allocation aligns with priorities.
 - **Objective:** Focus on clear, actionable outcomes.
 - **Follow-up:** Implement ongoing assessment and updates.

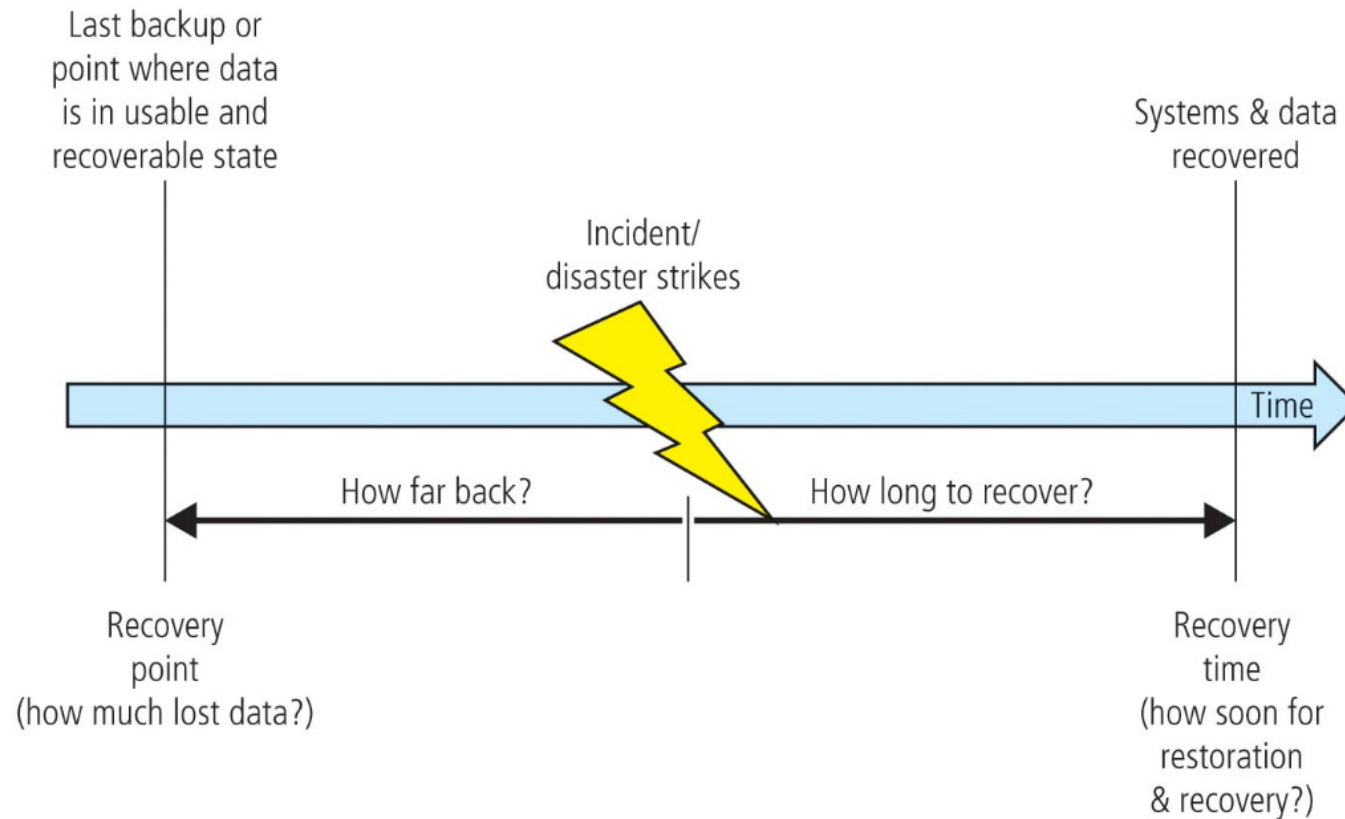
Business Process and Recovery Criticality

- First Major Task in BIA
 - Analyse and prioritize business processes based on their alignment with the organization's mission.
- Evaluation Approach
 - Assess each department, unit, or division independently to determine the importance of their functions.
- Tools for Evaluation
 - Weighted Analysis Table: Useful for evaluating business functions
 - BIA Questionnaire: Facilitates identification and collection of relevant information.

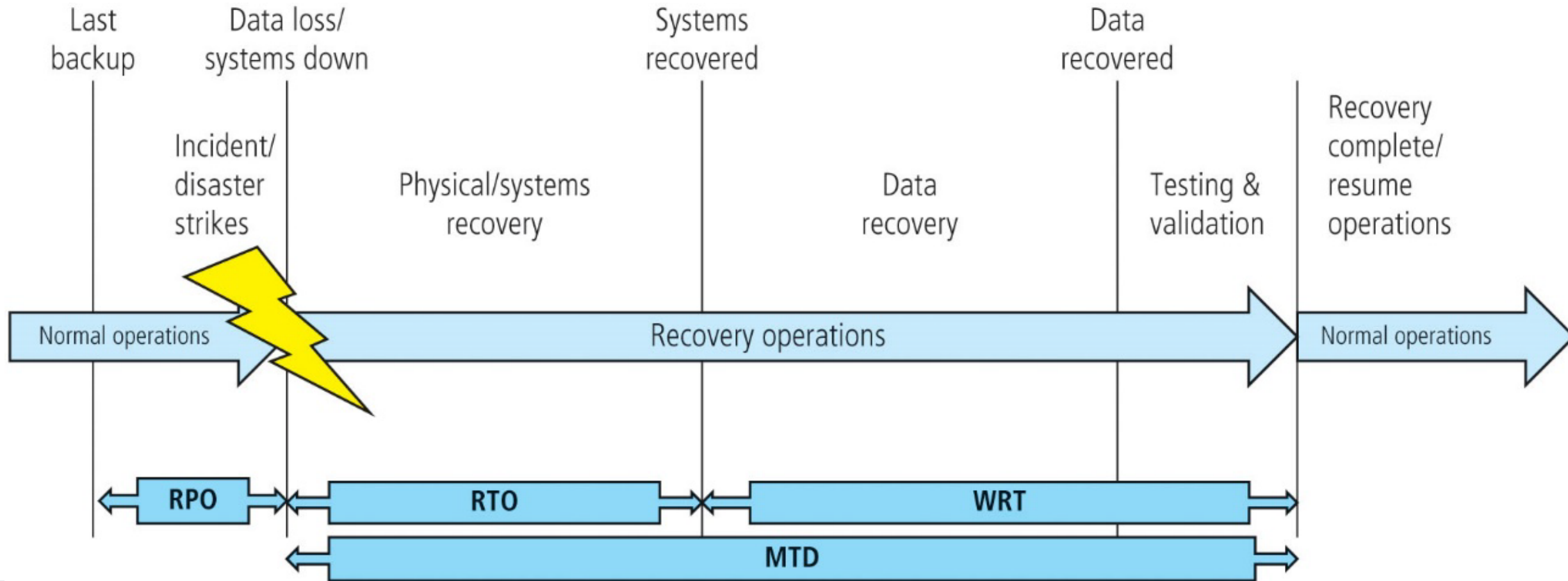
Business Process and Recovery Criticality

- Recovery Criticality in Organisations
 - Key measures focus on the amount of the asset to recover within a specific timeframe.
- Commonly Used Terms
 - **Recovery Time Objective (RTO)**: Maximum time to restore operations
 - **Recovery Point Objective (RPO)**: Maximum data loss acceptable
 - **Maximum Tolerable Downtime (MTD)**: Total time a process can be disrupted.
 - **Work Recovery Time (WRT)**: Time needed to transition back to full functionality
- **Cost Optimisation**: Plotting cost balance points helps identify the optimal trade-off between disruption and recovery costs .

RPO Vs RTO



RTO, RPO, MTD and WRT



Information Asset Prioritisation

- **BIA Assessment by CPMT:**
 - Evaluates priorities and relative values of mission/business processes.
 - Considers information assets used by these processes.
- **Influence of High-Value Information Assets:**
 - High-value assets may affect the valuation of business processes.
- **Connection to Risk Management:**
 - Typically performed as part of the risk-assessment function within the risk management process.

Recovery Requirements

- **Resource Planning Post-BIA:**
 - Determine resources required to recover prioritized mission/business processes and associated assets.
 - Identify and describe relevant resources for each process and information asset identified in the BIA stage.
- **Simplified Organisation Method:**
 - Use a resource/component table to organize and present this information effectively.

Recovery Requirements

•Resource Planning Post-BIA:

- Determine resources required to recover prioritized mission/business processes and associated assets.
- Identify and describe relevant resources for each process and information asset identified in the BIA stage.

•Simplified Organisation Method:

- Use a resource/component table to organize and present this information effectively.

•Final Stage of BIA:

- Prioritise resources linked to mission/business processes.

Mission/Business Process	Required Resource Components	Additional Resource Details	Description and Estimated Costs
Provide customer support (help desk)	Trouble ticket and resolution application	Application server w/LINUX OS, Apache server, and SQL database	Each help desk technician requires access to the organization's trouble ticket and resolution software application, hosted on a dedicated server. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk network segment	25 Cat5e network drops, gigabit network hub	The help desk applications are networked and require a network segment to access. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk access terminals	1 laptop/PC per technician, with Web-browsing software	The help desk applications require a Web interface on a laptop/PC to access. See current cost recovery statement for valuation.
Provide customer billing	Customized accounts receivable application	Application server with Linux OS, Apache server, and SQL database	Accounts Receivable requires access to its customized AR software and customer database to process customer billing. See current cost recovery statement for valuation.

Contingency Planning Policies

- Policy Development for CP Documents
 - Establish the policy environment to support the BIA process.
 - Provide policy guidance for creating planning components: IR, DR, and BC.
- Policy Guidance
 - Define subordinate team structures and organizational philosophy.
 - Assist in structuring the overall contingency plan.
- Role of Policies
 - Similar to enterprise InfoSec policies, each CP document is based on a specific policy.

Chapter 10 Planning for Contingencies

INCIDENT RESPONSE

Introduction to Incident Response

- IR involves detecting, reacting to, and recovering from incidents like attacks, errors, outages, and natural disasters.
- Importance of careful planning for quick containment and resolution by the Incident Response Planning Team (IRPT).

Key Incident Response Terminology

- **Adverse Events vs. Incidents:**
 - **Adverse event:** A potential threat to information assets.
 - **Incident:** Real threat affecting information, triggering the IR Plan.
- IR focuses on reactive measures but includes preventive recommendations.

IR and CPMT

- **Early Task of CPMT:**
 - Form the Incident Response Planning Team (IRPT).
 - Develop policy defining team operations and responses to incidents.
 - Advise users on contributing effectively to incident response.
- **Formation of CSIRT:**
 - IRPT establishes the Computer Security Incident Response Team (CSIRT).
- **NIST Cybersecurity Framework (CSF):**
 - Developed to enhance critical infrastructure cybersecurity protection.

Core Functions of the Framework

1. Identify:

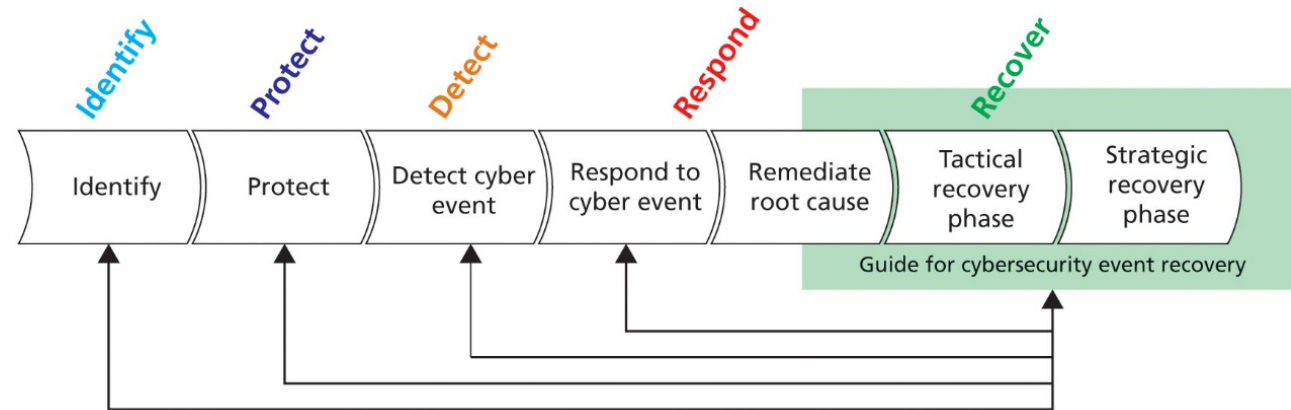
- Understand and manage cybersecurity risks to systems, assets, data, and capabilities.

2. Protect:

- Implement safeguards to ensure the delivery of critical services.

3. Detect:

- Develop activities to identify cybersecurity events promptly.



4. Respond:

Take action to mitigate the impact of detected cybersecurity events.

5. Recover:

Restore capabilities or services impaired by cybersecurity events.

Creating the IR Plan

- Responsibility of CISO or IT manager with security duties.
- **Core Elements (NIST SP 800-61):**
 - Mission, goals, and senior management approval.
 - Team communication, metrics, and roadmap for IR capability.
 - Integration within organizational structure.
- The IR teams responsible for developing & executing the plan
 - **IRPT:** Develops predefined responses and guides through IR steps.
 - **CSIRT:** Executes the IR plan with technical and managerial expertise.
- Roles: Diagnose, react, prevent, and recover from incidents.

NIST Framework for IR Policy components

- Management commitment, policy objectives, and scope.
- Incident definitions, organisational roles, severity ratings, and performance measures.
- The Incident Response lifecycle includes:

1.Preparation:

Establish policies, procedures, and tools to proactively address incidents.

2.Detection & Analysis:

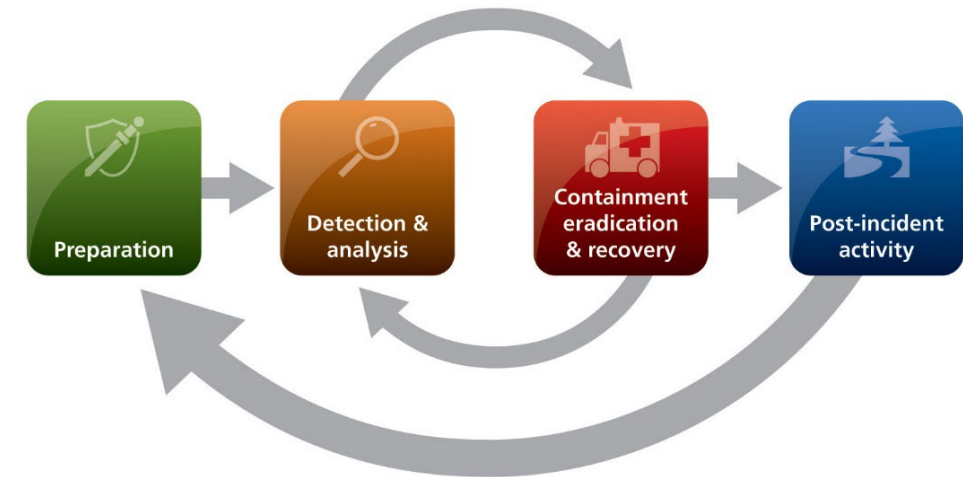
Identify and evaluate potential incidents, determining their scope and severity.

3.Containment, Eradication & Recovery:

Take action to stop the incident, remove its root cause, and restore systems.

4.Post-Incident Activity:

Analyse the response process to improve future incident management.



Incident Response Planning

- When a threat becomes a valid adverse event, it is classified as an InfoSec incident if:
 - It is directed against information assets
 - It has a realistic chance of success
 - It threatens the confidentiality, integrity, or availability of information resources and assets
- It is important to understand that IR is a reactive measure, not a preventative one, although most IR plans include preventative recommendations

Incident Response Actions

- Incident response actions can be organized into three basic phases:
 - **Detection:** Determine actual incidents via indicators and classification.
 - **Reaction:** Stop the incident, mitigate effects, and regain control.
 - **Recovery:** Assess damage, resolve vulnerabilities, restore operations.

Detecting and Classifying Incidents

- **Incident Indicators:**
 - Possible: Unfamiliar files, unusual system crashes.
 - Probable: Unexpected activities, new accounts, intrusion reports.
 - Definite: Dormant accounts, changes to logs, notifications.
- **Classification:** Distinguish routine events from actual incidents.

Containment and Recovery Strategies

- **Containment Tasks:**

- Disable compromised accounts, reconfigure firewalls, stop compromised services.

- **Recovery Steps:**

- Assess damage, restore systems and data, address vulnerabilities, and monitor systems.

Common IR Challenges

- Lack of clear command, incomplete plans, and insufficient documentation.
- Failing to distinguish containment from remediation or ensuring effective monitoring.

Chapter 10: Planning for Contingencies

DISASTER RECOVERY

Disaster Recovery

- Disaster recovery planning (DRP) entails preparation for and recovery from a disaster, whether natural or man-made
- In general, an incident is a disaster when:
 - the organization is unable to contain or control the impact of an incident, or
 - the level of damage or destruction from an incident is so severe the organization is unable to quickly recover
- The key role of a DR plan is defining how to reestablish operations at the location where the organization is usually

Disaster Recovery (Continued)

- As you learned earlier, the CP team creates the DR planning team (DRPT)
- The DRPT in turn organizes and prepares the DR response teams (DRRTs) to actually implement the DR plan in the event of a disaster
- These teams may have multiple responsibilities in the recovery of the primary site and the reestablishment of operations:
 - Recover information assets that are salvageable from the primary facility after the disaster
 - Purchase or otherwise acquire replacement information assets from

Disaster Recovery Response Teams

- Some common DRRTs include:
 - DR Management
 - Communications
 - Computer Recovery (Hardware) Team
 - Systems Recovery (OS)
 - Network Recovery Team
 - Storage Recovery
 - Applications Recovery
 - Data Management
 - Vendor Contact
 - Damage Assessment and Salvage
 - Business Interface
 - Logistics
 - Others (as needed)

Disaster Recovery Process

- The NIST methodology can be adapted for DRP:
 - Organize the DR team
 - Develop the DR planning policy statement
 - Review the BIA
 - Identify preventive controls
 - Create DR strategies
 - Develop the DR plan document
 - Ensure DR plan testing, training, and exercises

Disaster Recovery Policy (Continued)

- The DR team, led by the manager designated as the DR team leader, begins with the development of the DR policy soon after the team is formed
- The DR policy contains the following key elements:
 - Purpose
 - Scope
 - Roles and responsibilities
 - Resource requirements
 - Training requirements
 - Exercise and testing schedules

Disaster Classifications

- A DR Plan can classify disasters in a number of ways:
 - Natural disasters
 - Man-made disasters
- By speed of development
 - Rapid onset disasters
 - Slow onset disasters

Natural Disasters

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornado or severe windstorm
- Hurricane or typhoon
- Tsunami
- Electrostatic discharge (ESD)
- Dust contamination

Planning to Recover

- Scenario development and impact analysis are used to categorize the level of threat of each potential disaster
- When generating a DR scenario, start with the most important asset: people
- Key points in the DR plan:
 - Clear delegation of roles and responsibilities
 - Execution of the alert roster and notification of key personnel
 - Clear establishment of priorities
 - Documentation of the disaster
 - Action steps to mitigate the impact



Simple DR Plan Elements

- Name of agency
- Date of completion or update of the plan and the date of the most recent test
- Agency staff to be called in the event of a disaster
- Emergency services to be called (if needed) in event of a disaster
- Locations of in-house emergency equipment and supplies
- Sources of off-site equipment and supplies

Chapter 10: Planning for Contingencies

BUSINESS CONTINUITY

Business Continuity Planning (BCP)

- **Definition:** Business Continuity ensures critical business functions continue during catastrophic incidents or disasters.
- **BCP Activation:** Executed alongside Disaster Recovery Plan (DRP) when needed.
- **Key Focus:** BC addresses alternative site operations, while DRP focuses on reestablishing the primary site.

NIST Methodology for BC Planning

- **Steps to Develop BC Plan:**

- Form the BC Team.
- Develop BC policy statement.
- Review the Business Impact Analysis (BIA).
- Identify preventive controls.
- Create relocation strategies.
- Develop BC plan and conduct testing, training, and maintenance.

- **Policy Key Elements:**

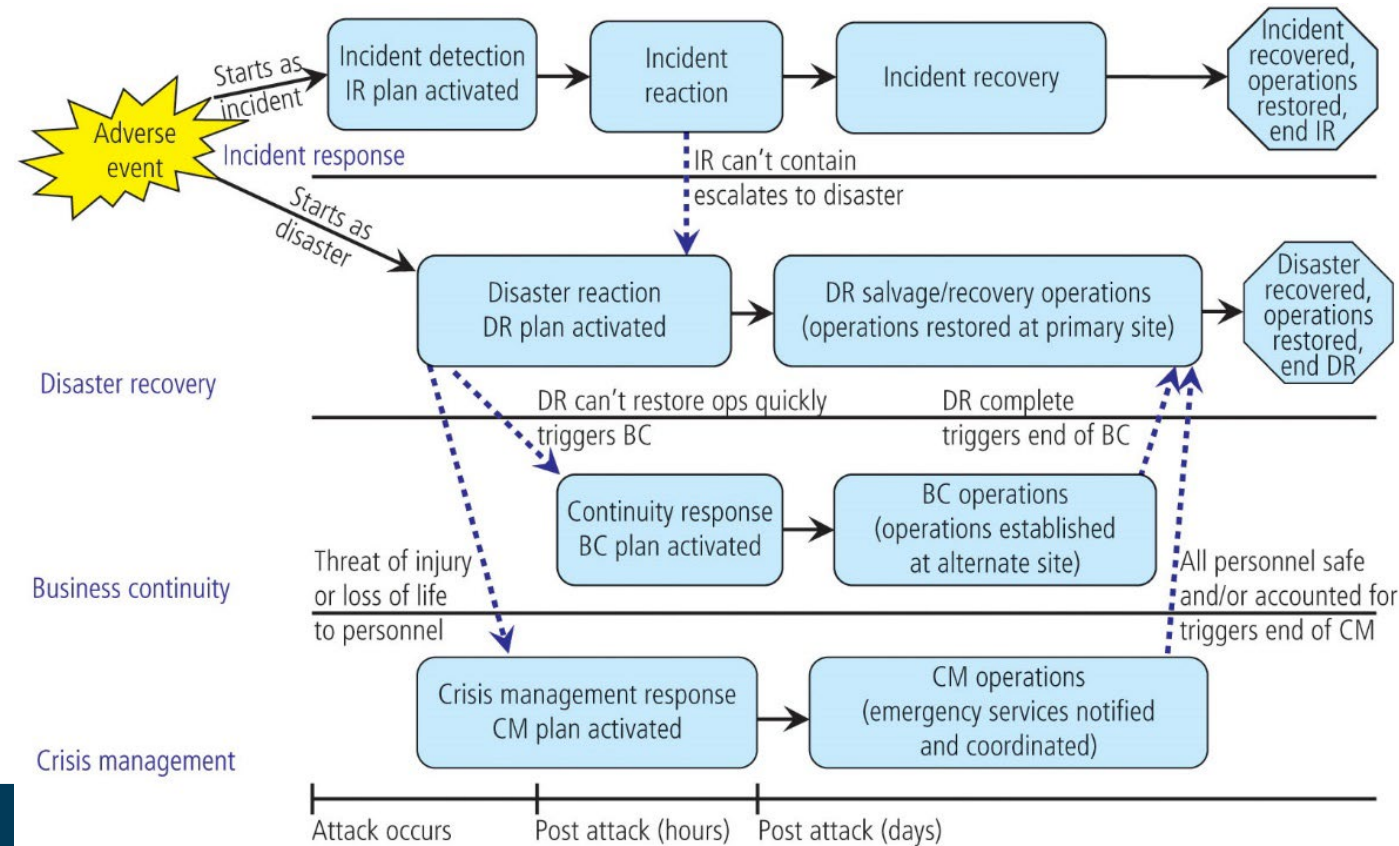
- Purpose, scope, roles, resource requirements, training, and testing schedules.

Continuity Strategies

- **Exclusive-Use Options:**
 - **Hot Sites:** Fully operational alternate sites.
 - **Warm Sites:** Partially equipped sites requiring setup.
 - **Cold Sites:** Basic infrastructure requiring full setup.
- **Shared-Use Options:**
 - Timeshare, service bureaus, mutual agreements.
- **Specialised Options:**
 - Rolling mobile sites, externally stored resources.

Continuity Strategies

- There are several continuity strategies for business continuity; determining factor is usually cost
- Three exclusive-use options:
 - Hot sites
 - Warm sites
 - Cold sites
- Three shared-use options:
 - Timeshare
 - Service bureaus
 - Mutual agreements
- Specialized options:
 - Rolling mobile site
 - Externally stored (prepositioned) resources



Chapter 10: Planning for Contingencies

CRISIS MANAGEMENT

Crisis Management (CM)

- **Focus of CM:** Addresses disaster effects on people, organizational image, and public communication.
- **Key Roles of the CM Team (According to Gartner Research):**
 - Support personnel during the crisis.
 - Keep the public informed and ensure recovery communication.
 - Manage communication with key stakeholders like customers, suppliers, and media.

Crisis Management Team (CMT)

- **Primary Tasks:**
 - Verify personnel status.
 - Activate the alert roster.
 - Coordinate with emergency services.
- **Base of Operations:** Establish command center near the disaster site.
- **Inclusivity:** Team should include representatives from all functional areas.

References

- Slides are devised from the recommended books:
 - Whitman, M.E.,Mattord, H.J., Principles of Information Security . Cengage Learning 658.
 - Management of Information Security 6th Ed by Whitman & Herbert
 - Chapter 10: Planning for Contingencies



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk