Business Continuity and Disaster Recovery

Week 5 – Risk Assessment

Week 5: Chapter 5 Outline

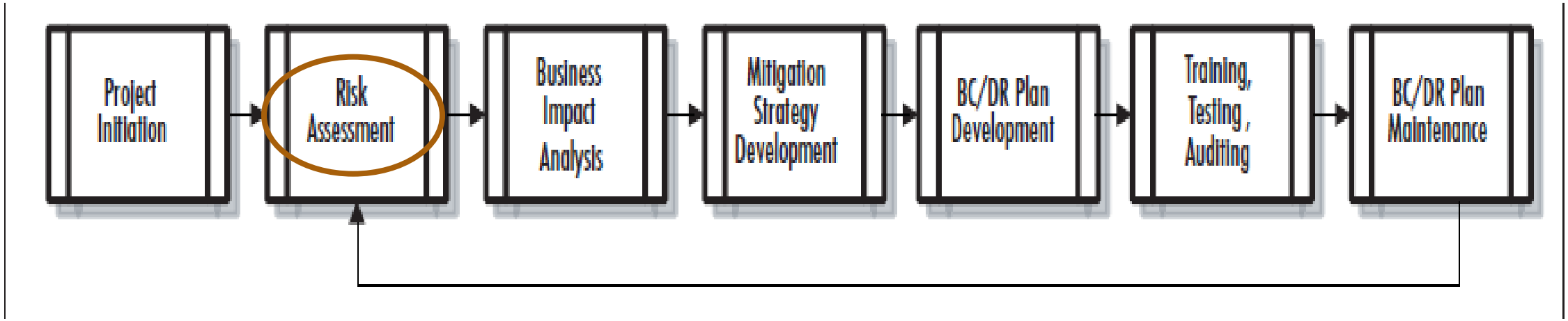
RECAP FROM WEEK 4

- Elements of project success
- Project plan components
- Key contributors and responsibilities
- Project definition
- Business continuity and disaster recovery plan

WEEK 5

- Risk management basics
- People, Process, Technology and Infrastructure in Risk Management
- IT Specific Risk Management
- Risk assessment components
- Threat assessment methodology
- Vulnerability assessment

Basic Steps in BCDR Plan



Risk Management Vocabulary (Conklin, 2016)

Risk is the possibility of suffering harm or loss.

Risk management is the overall decision-making process of:

- Identifying threats and vulnerabilities and their potential impacts
- Determining the costs to mitigate such events
- Deciding what actions are cost effective for controlling these risks

Risk assessment (or **risk analysis**) is the process of:

- Analyzing an environment to identify the risks (threats and vulnerabilities)
- Mitigating actions to determine (either quantitatively or qualitatively) the impact of an event that would affect a project, program, or business

An **asset** is any resource or information an organization needs to conduct its business.

Risk Management Vocabulary (Conklin, 2016)

A **threat** is any circumstance or event with the potential to cause harm to an asset.

A **threat actor** (agent) is the entity behind a threat.

A **threat vector** is a method used to affect a threat.

- Example: a virus/worm (threat) that is delivered via a USB pen drive (vector).

A **vulnerability** is any characteristic of an asset that can be exploited by a threat to cause harm.

Impact is the loss (or harm) resulting when a threat exploits a vulnerability.

A **control** is a measure taken to detect, prevent, or mitigate the risk associated with a threat.

- Also called **countermeasure** or **safeguard**

WHICH ONE IS A THREAT/VULNERABILITY?

Introduction

The concept and practical application of risk management into:

- the broad business perspective
- the practical business continuity and disaster recovery planning perspective
- the IT-centric perspective

We cannot create a viable BC/DR plan until we know which specific THREATS the company faces.

Common threats faced by organizations:

- People – insider threats
- Process – security policies are not enforced – affect employees' non-compliance
- Technology – server failure or power outage

Threats can be unique to a particular organization – for e.g. foreign intelligence in a government agency

Risk Management Basics (1 of 2)

Risk management - How all risks are managed across the enterprise

Financial risks to publicly traded companies

- Risks to the value of their company through the stock market, shareholder lawsuits for mismanagement of the company, and they also face risks based on currency fluctuations in an international trading environment

Risks associated with products:

- Product tampering, product malfunction, product contamination

Risk to loss of life in healthcare or utility companies (example?)

Business risk is defined as:

- The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect businesses. It includes risk analysis, cost benefit analysis, selection, implementation, and testing of selected strategies, and maintenance of those strategies over time.

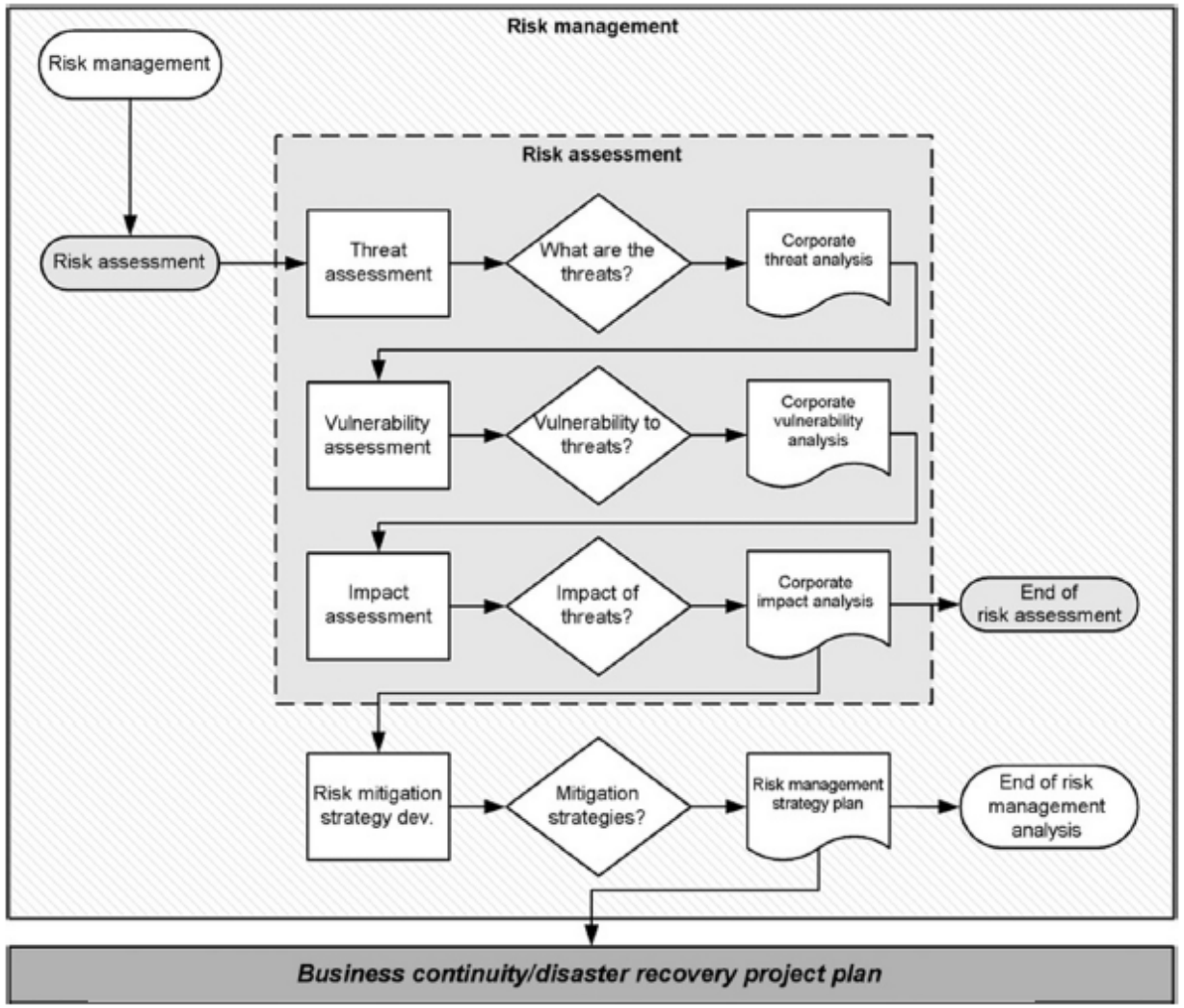
Risk Management Basics (2 of 2)

Three key aspects to any risk assessment methodology

1. The risk assessment process—how you go about performing the assessment.
2. The assessment approach—will you opt for a quantitative, qualitative, or hybrid approach? You need to select an approach and use it consistently.
3. Risk analysis approach – focus on threat, asset or impact? Or all three? Be consistent.

Four basic steps in risk management:

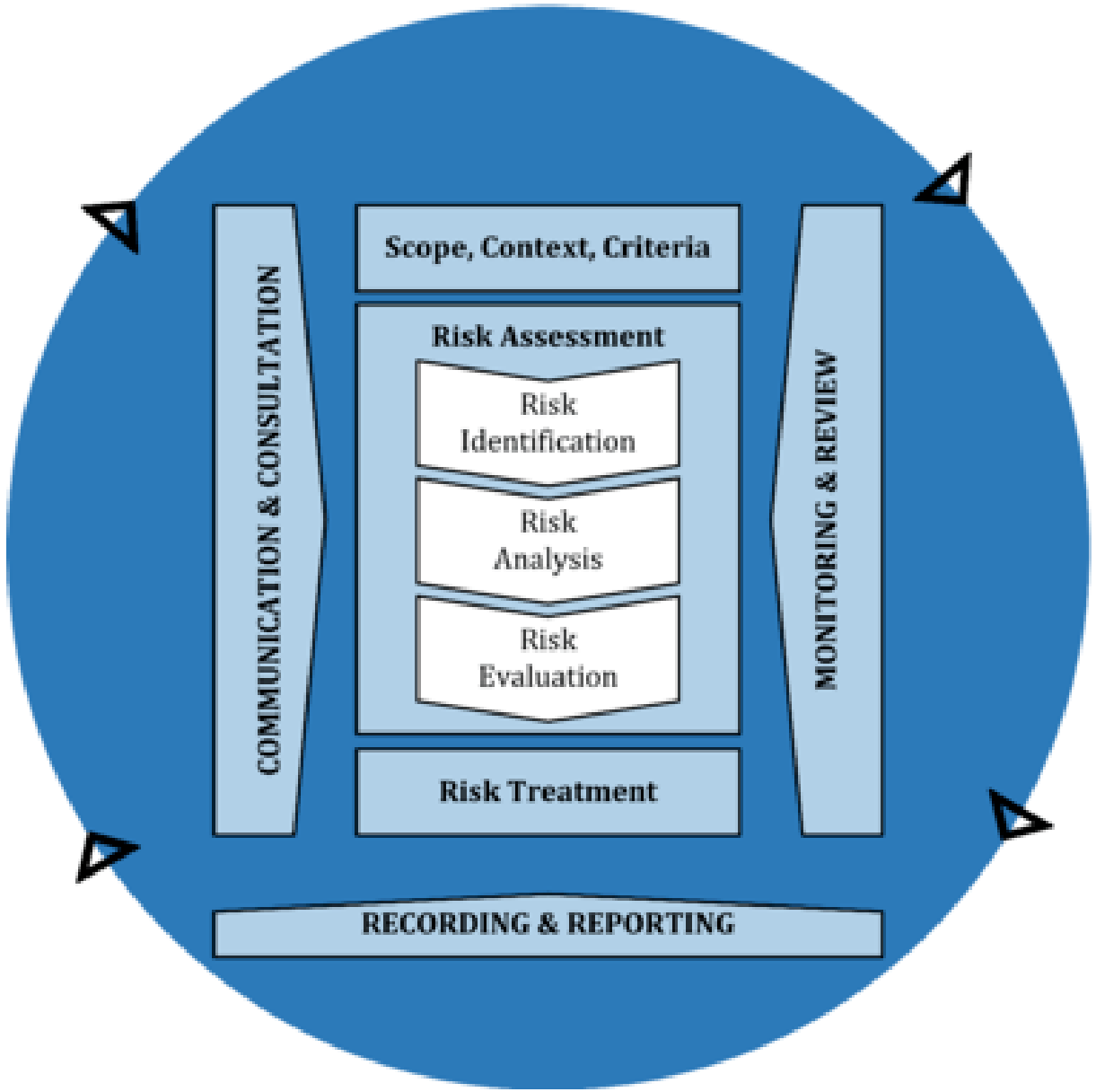
1. Threat assessment
2. Vulnerability assessment
3. Impact assessment
4. Risk mitigation strategy development


Risk management
Risk management
Risk assessment
Risk assessment
Threat assessment
What are the threats?
Corporate threat analysis
Vulnerability assessment
Vulnerability to threats?
Corporate vulnerability analysis
Impact assessment
Impact of threats?
Corporate impact analysis
End of risk assessment
Risk mitigation strategy dev.
Mitigation strategies?
Risk management strategy plan
End of risk management analysis
Business continuity/disaster recovery project plan

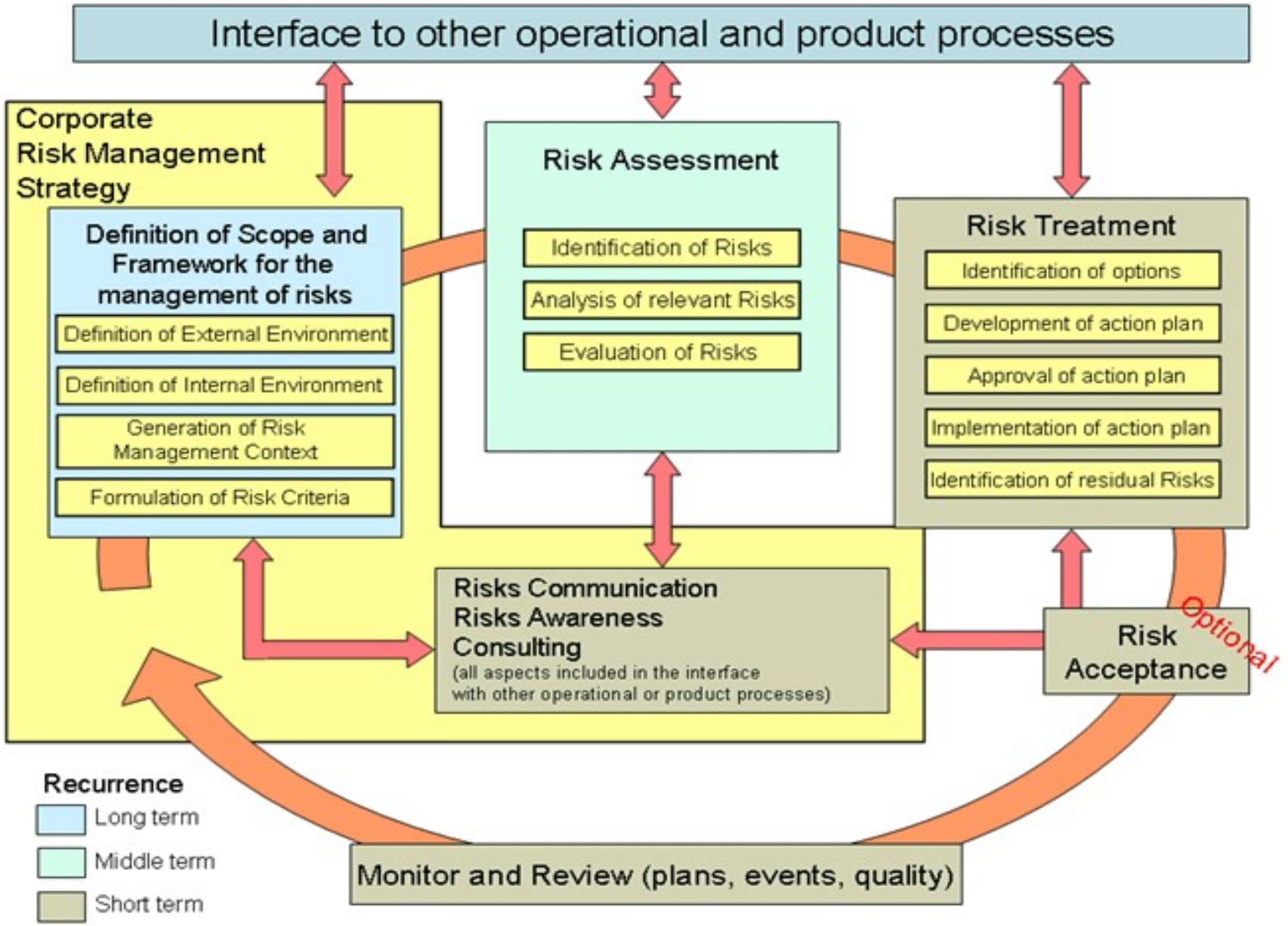
Risk Management Standards

ISO 31000:2018 Risk management — Guidelines

ISO 27005 Information Security Risk Management



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY



IT-centric View of Risk Management

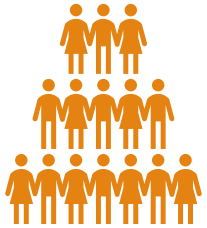
National Institute of Standards and Technology
U.S. Department of Commerce

"Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

The objective of performing risk management is to enable the organization to accomplish its mission(s)

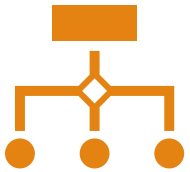
- (1) by better securing the IT systems that store, process, or transmit organizational information;
- (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and
- (3) by assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.



People

If the power goes out in the building, how likely is it that people will be able to get anything done?

People respond in a variety of ways to small and large events.



Process

If the company has any processes still done by people without technology, those processes can proceed but sooner or later, those processes will require computer data as input or output.

Technology

What happen when the Internet is out?

Technology is needed so that the people in the company can use the processes defined to conduct business

Technology is most often useless without the context of people and process

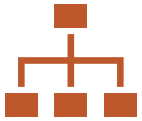
People, Process, Technology and Infrastructure in Risk Management (1 of 2)

People, Process, Technology and Infrastructure in Risk Management (2 of 2)

Infrastructure

- IT infrastructure (what are the components of IT infra?)
- From an organizational standpoint:
  - Internal: the building and facilities, the utilities coming into the building
  - External: public transportation, public utilities, communication services, local, state, or national resources pertinent to your business
- Who should manage the risks to internal infrastructure?
- Who should manage the risks to external infrastructure?

IT-Specific Risk Management



IT-specific risk management is a subset of overall business risk management

As an IT professional, your job is to ensure that the organization understands IT risks and supports efforts to mitigate those risks.

Objectives

Securing IT systems

Enabling management to make well-informed decisions with regard to the purchasing and implementation of IT systems

Enabling management to authorize the IT systems on the basis of supporting documentation that results from the IT risk management activities

The IT risk assessment process intersects with BCDR planning risk assessment in that we need to evaluate the various risks to the company and the IT systems

However, the goals are the same: to enable businesses to meet their strategic objectives.

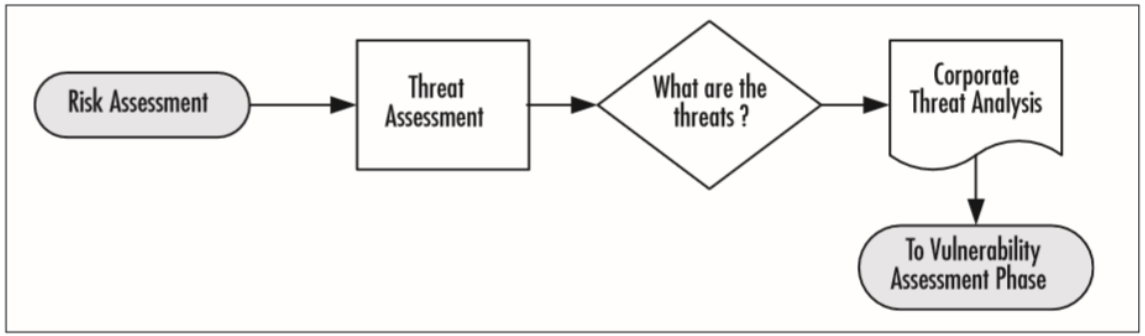
Risk Assessment Components

THREAT ASSESSMENT

VULNERABILITY ASSESSMENT

IMPACT ASSESSMENT

Threat Assessment



Risk Assessment begins with Threat Assessment: the assessment of all potential threats and an analysis of those threats

In BC/DR planning, understanding the threats and threat sources can help you uncover potential risks to your company or IT systems about which you were previously unaware

- E.g. of a Threat – power outage in the data centre
- E.g. of Threat sources – transformers are struck by lightning or when substations or the power grid itself experience some major failure of the power infrastructure

Threat Assessment

Information gathering methods - to gather data about your company's risks:

- Questionnaires
- Interviews with subject matter experts
- Document reviews
- Research – study natural disasters in your area – collect data from local fire departments, police departments

Identify potential disasters:

- Natural: floods, haze,
- Health: pandemic
- Man-made: human threats = theft, sabotage, vandalism, labour disputes, workplace violence, terrorism, cyber threats.
- Infrastructure threats:
  - Building-specific failures (structural damage, systems failures),
  - Public transportation disruption (roads, railways, airports),
  - Loss of utilities (power grid failure, gas supply failure, water supply failure),
  - Petroleum or oil shortage, Food or water contamination, Regulatory or legal changes

Threat Assessment

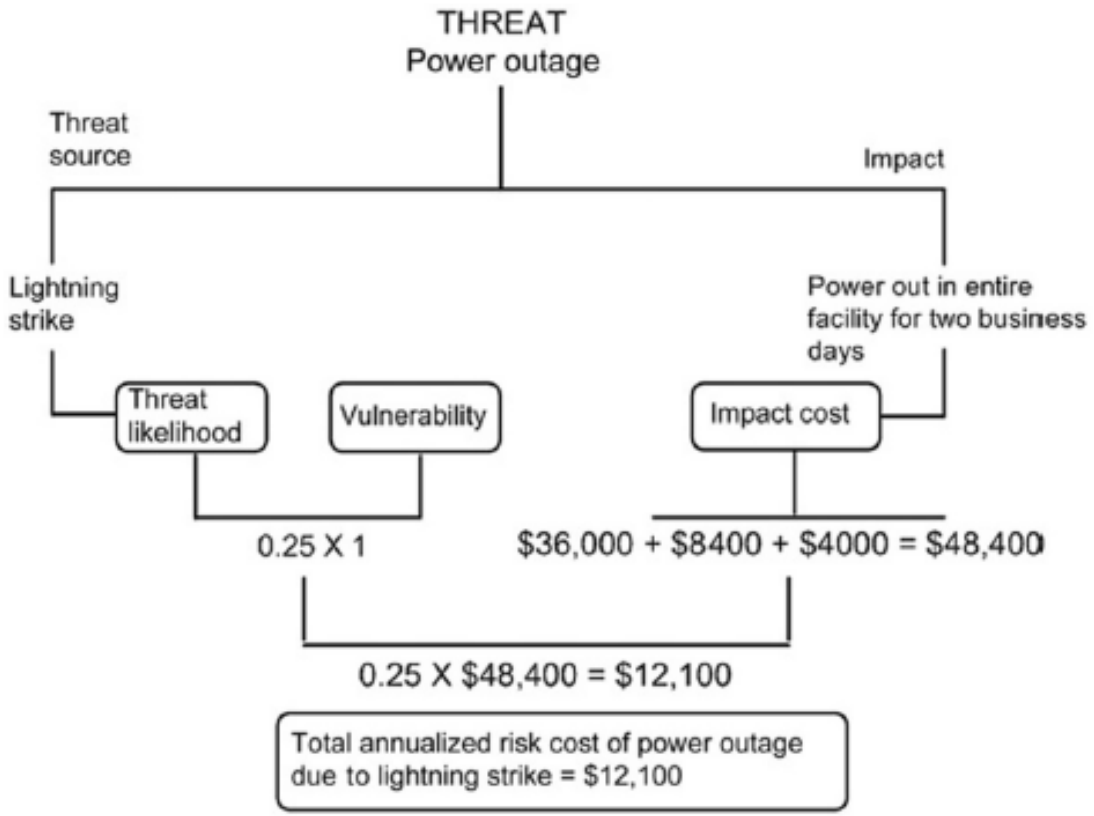
FIGURE 4.5

Deliverable from threat source assessment.

Table 4.4 Risk Assessment Table

Item No	Threat Name	Threat Source	Vulnerability Rating	Likelihood Rating	Existing Controls	Impact Rating	Overall Risk Rating
001	Fire	Internal					
002		External					
003	Flood	Internal					

Threat Assessment Methodology (1 of 2)



Quantitative approach

- use numbers to represent threats, vulnerabilities, and impacts.

A quantitative assessment can be defined as observations that involve measurements and numbers.

If you know that your annualized risk cost for a power outage from a lightning strike is $12,100, would you spend

- $10,000 backup power generator?
- $5000 to install power equipment?
- $1000/year insurance rider to cover utilities outage?

Remember, you can accept, avoid, reduce, or transfer risk

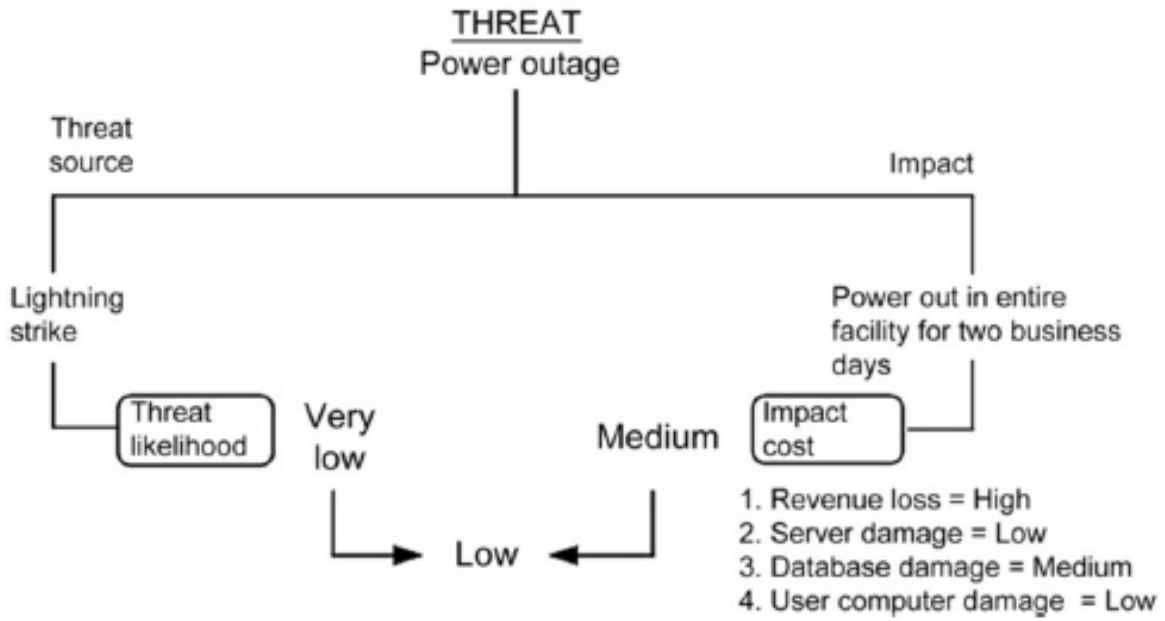
Threat Assessment Methodology (2 of 2)

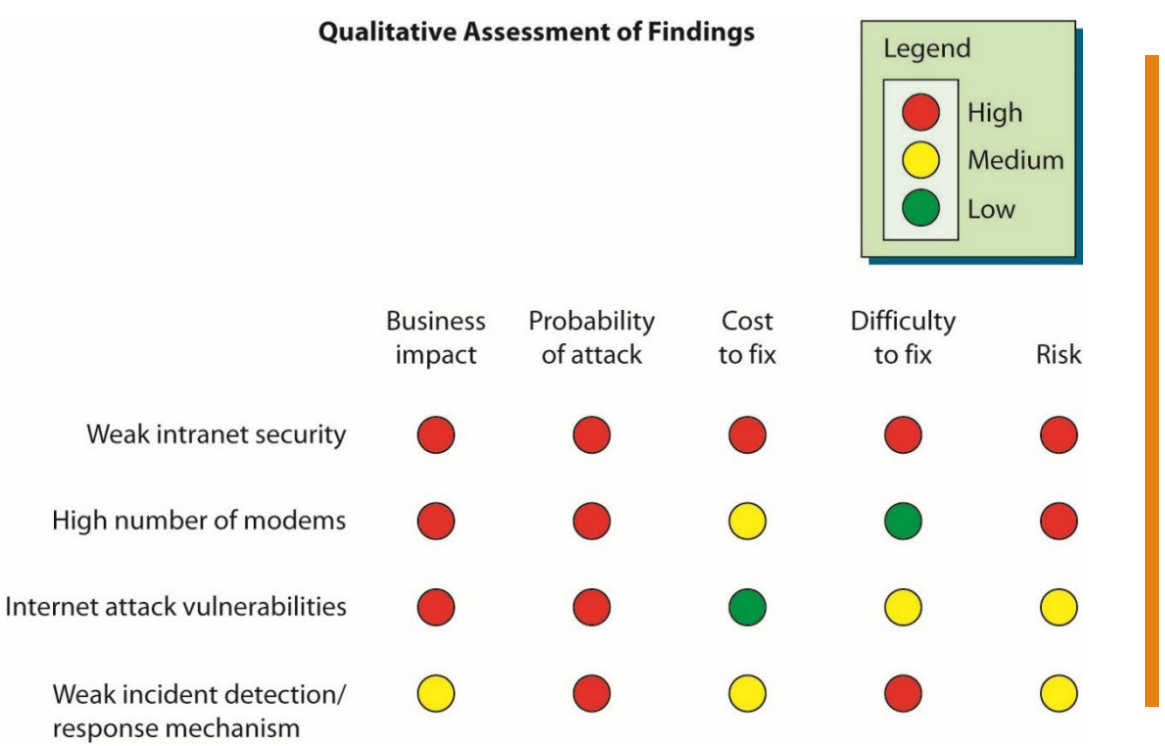
Qualitative assessments use words or relative values to express risk, cost, and impact.

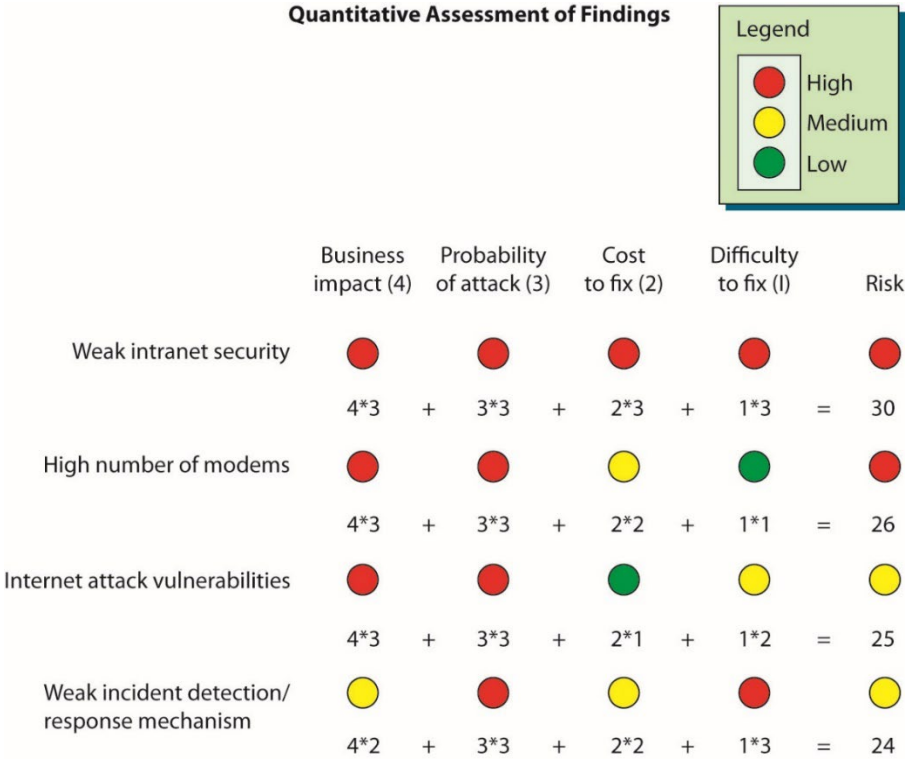
The first step in using a qualitative system is to define the scale you want to use and then use it consistently

Table 4.6 NIST Likelihood Matrix

Likelihood Level	Description
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised



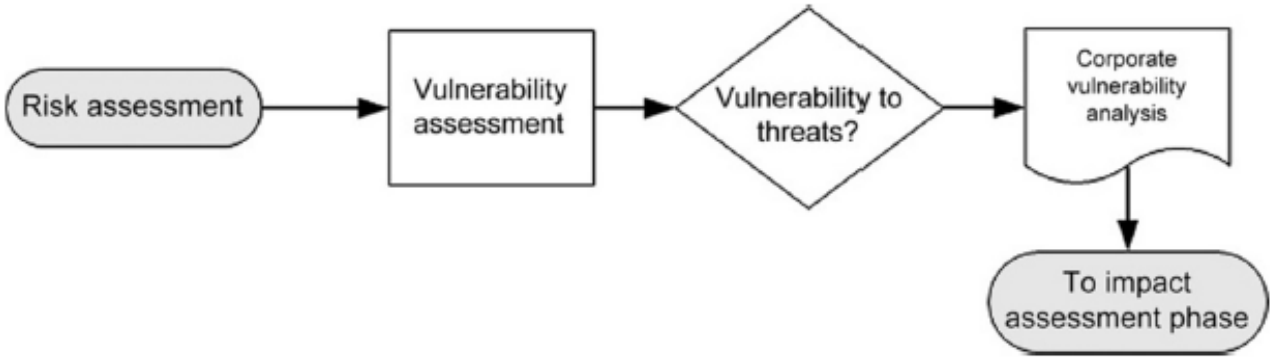




QUALITATIVE VS. QUANTITATIVE

Vulnerability Assessment

- A vulnerability is defined as the weakness, susceptibility, or exposure to hazards or threats.
- A software program vulnerability is a weakness that poses a problem if discovered and exploited.
- Vulnerabilities in the case of BCDR are the various areas of the business and IT systems that are exposed or susceptible to the threats defined in the previous assessment phase.
- Vulnerabilities can be exploited intentionally or triggered unintentionally.



System Vulnerabilities

Analyzes how vulnerable, susceptible, and exposed a business or system is to a particular threat

It should include an assessment of how vulnerable a particular system is to a threat as well as the likelihood of that threat occurring.

For e.g. a server that is outside the firewall is far more vulnerable to external attacks than a server inside the firewall

Vulnerabilities are characteristics of an asset that can be exploited by a threat to cause harm.

- Not all errors or bugs are vulnerabilities.
- For an error or bug to be classified as a vulnerability, it must be exploitable—an attacker must be able to use the bug to cause a desired result.

Three elements needed for a vulnerability to occur:

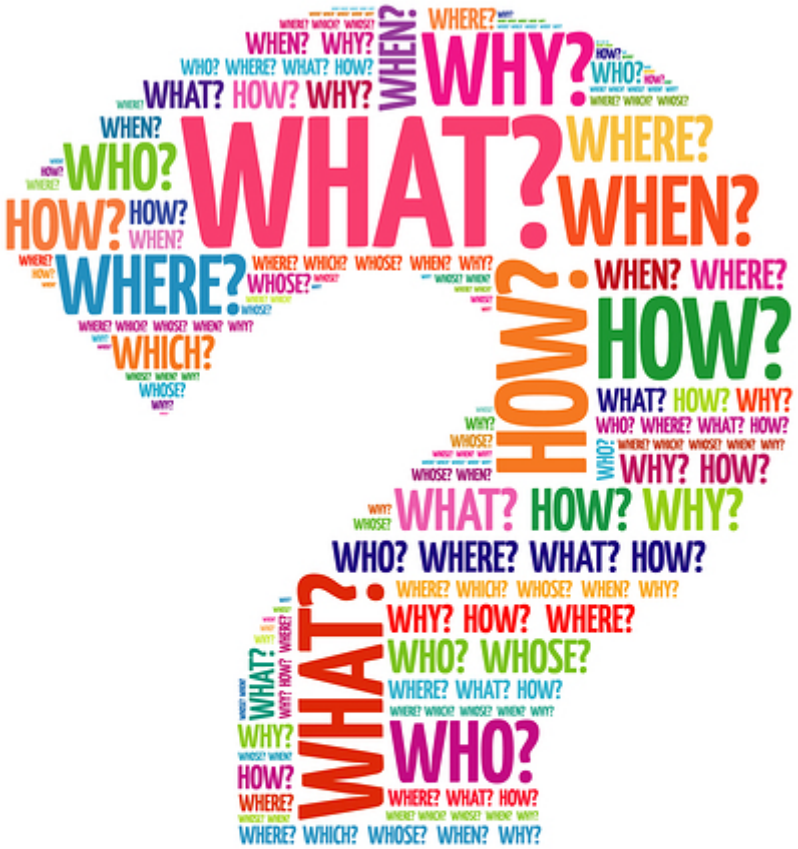
- The system must have a flaw.
- The flaw must be accessible by an attacker.
- The attacker must possess the ability to exploit the flaw.

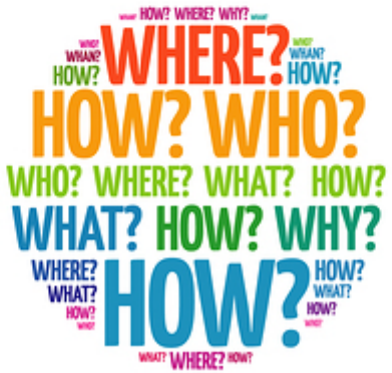
Impact Assessment

- Assess the potential impact through the BIA.
- We will cover BIA in the next chapter.

Risk Assessment Exercise

Get into your group. Walk around KICT and look at any threat and risk. Take a picture of the threat/risk. Make a risk assessment table (refer to slide no. 21). Submit it in the next class on the 18th April 2024.


WHEN? WHY?
WHERE?
WHY?
WHO?
WHAT? HOW? WHY?
WHEN?
WHO?
WHAT?
WHERE?
HOW?
HOW?
WHEN?
WHERE?
WHEN? WHERE?
WHICH?
WHOSE?
HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHY? HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHERE? WHICH? WHOSE? WHEN? WHY?
WHY? HOW? WHERE?
WHO? WHOSE?
WHERE? WHAT? HOW?
WHAT?
WHY?
WHO?
HOW?
WHERE?
WHERE? WHAT? HOW?
WHERE? WHICH? WHOSE? WHEN? WHY?


WHERE?
HOW? WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
HOW?


Questions