REVA UNIVERSITY

Established as per the Section 2(f) of the UGC Act, 1956
Approved by AICTE, COA and BCI, New Delhi

Lecture 1.2
Planning for Security

School of Computing and Information Technology

Introduction Class

Recap of previous Lecture

RECAP OF PREVIOUS LECTURE

- Importance of Information and Network Security
- Course Description
- Course Objectives
- Course Contents

SOFTWARE ENGINEERING RELATED COMPANIES

THE HISTORY OF INFORMATION SECURITY

- ✓ The history of information security begins with computer security. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats— arose during World War II when the first mainframes, developed to aid computations for communication code breaking were put to use.

- ✓ Multiple levels of security were implemented to protect these mainframes and maintain the **integrity of their data**. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

INTRODUCTION

- ✓ An organization’s information security effort succeeds only if it operates in conjunction with the organization’s information security policy.
- ✓ An information security program begins with policy, standards, and practices, which are the **foundation** for the information security architecture and blueprint.
- ✓ The creation and maintenance of these elements require coordinated planning. the role of planning in the modern organization is hard to overemphasize.
- ✓ All but the smallest organizations engage in some planning: **strategic planning** to manage the allocation of resources and **contingency planning** to prepare for the uncertainties of the business environment

PLANNING FOR SECURITY

- ✓ Strategic planning sets out the **long-term direction** to be taken by the whole organization and by each of its component parts. Strategic planning should **guide organizational efforts and focus resources** toward specific, clearly defined goals.

- ✓ After an organization develops a general strategy, it **generates an overall strategic plan** by extending that general strategy into strategic plans for major divisions.

- ✓ Each level of each division then **translates** those plan objectives into more specific objectives for the level below.

PLANNING FOR SECURITY

- ✓ To execute this broad strategy and turn the **general strategy into action**, the executive team (sometimes called the C-level of the organization, as in CEO, COO, CFO, CIO, and so on) must first define individual responsibilities.

- ✓ The conversion of goals from one strategic level to the next lower level is perhaps more art than science.

- ✓ It relies on an executive's ability to know and understand the strategic goals of the entire organization, to know and appreciate the strategic and tactical abilities of each unit within the organization, and to negotiate with peers, superiors, and subordinates.

- ✓ This mix of skills helps to achieve the proper balance between goals and capabilities.

WHAT IS INFORMATION SECURITY (INFOSEC)?

✓ Information Security, sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information **risk management.**

Definition of Policy

A policy is a **plan or course of action** that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties. Policies are **organizational laws** in that they dictate acceptable and unacceptable behavior within the organization.

- ❖ Like laws, policies define what is right.
- ❖ what is wrong.
- ❖ what the penalties are for violating policy and
- ❖ what the appeal process is.

TYPES POLICIES

An information security policy provides rules for the protection of the information assets of the organization

Management must define three types of security policy, according to the National Institute of Standards

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

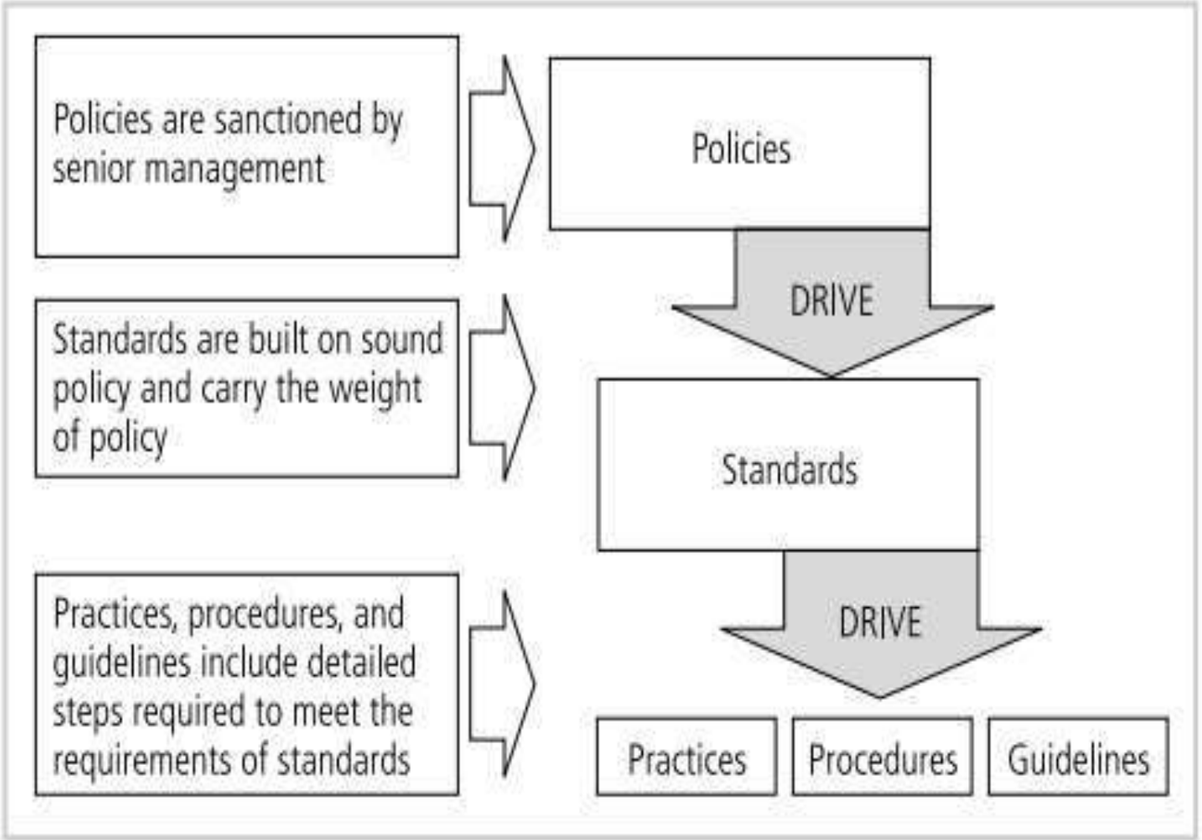


Figure 5-1 Policies, Standards, and Practices

DEFINITION OF STANDARDS

- ✓ Standards are more **detailed statements of what must be done to comply with policy.** They have the same requirements for compliance as policies.

- ✓ Standards may be informal or part of an organizational culture, as in de facto standards.
- ✓ Or standards may be published, scrutinized, and ratified by a group, as in formal or de jure standards.

- ✓ Finally, practices, procedures, and guidelines effectively explain how to comply with policy.

- ✓ Practices : Implementing standards and policies.

THE INFORMATION SECURITY BLUEPRINT

- ✓ After the information security team has inventoried the organization's information assets and assessed and prioritized the threats to those assets, it must conduct a series of risk assessments using quantitative or qualitative analyses, as well as feasibility studies and cost benefit analyses.

- ✓ These assessments, which include **determining each asset's current protection level,** are used to decide whether or not to proceed with any given control. Armed with a general idea of the vulnerabilities in the information technology systems of the organization, the security team develops a design blueprint for security, which is used to implement.

THE INFORMATION SECURITY BLUEPRINT

- ✓ It is the basis for the design, selection, and implementation of all security program elements including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program.

- ✓ The security blueprint, built on top of the organization's information security policies, is a scalable, upgradeable, comprehensive plan to meet the organization's current and future information security needs.

THE INFORMATION SECURITY BLUEPRINT

To select a methodology in which to develop an information security blueprint, you can adopt a published information security model or framework.

This framework can outline steps to take to design and implement information security in the organization.

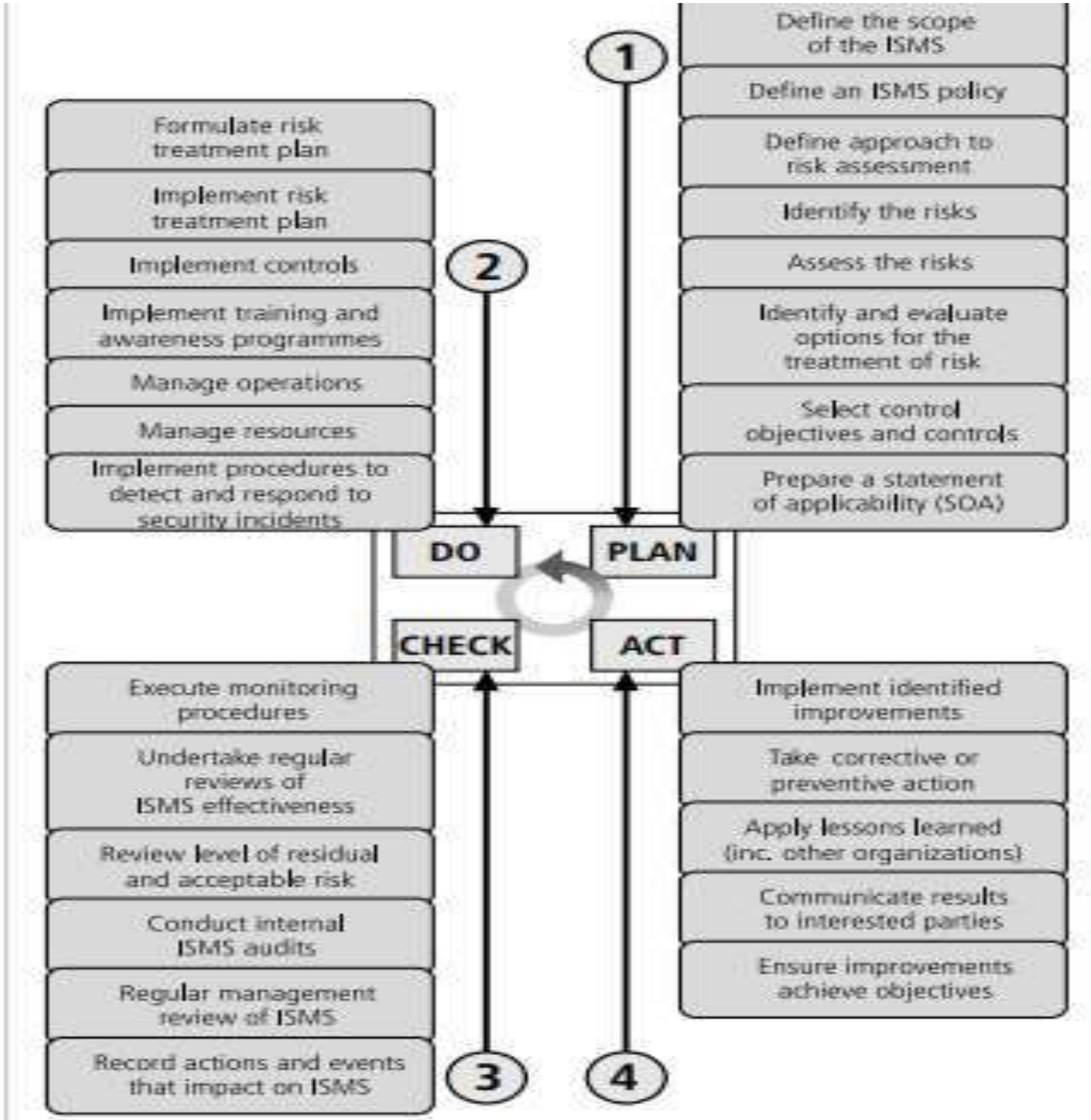
1.	Risk Assessment and Treatment
2.	Security Policy
3.	Organization of Information Security
4.	Asset Management
5.	Human Resource Security
6.	Physical and Environmental Security
7.	Communications and Operations
8.	Access Control
9.	Information Systems Acquisition, Development and Maintenance
10.	Information Security Incident Management
11.	Business Continuity Management
12.	Compliance

THE INFORMATION SECURITY BLUEPRINT

The ISO(International Standards Organization) 27000 Series security models

The stated purpose of ISO/IEC 27002 is to “give recommendations for information security management for use by those who are responsible for **initiating, implementing, or maintaining security in their organization.**

It is intended to provide a **common basis for developing** organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”


1
Define the scope of the ISMS
Define an ISMS policy
Define approach to risk assessment
Identify the risks
Assess the risks
Identify and evaluate options for the treatment of risk
Select control objectives and controls
Prepare a statement of applicability (SOA)
2
Formulate risk treatment plan
Implement risk treatment plan
Implement controls
Implement training and awareness programmes
Manage operations
Manage resources
Implement procedures to detect and respond to security incidents
DO
PLAN
CHECK
ACT
Execute monitoring procedures
Undertake regular reviews of ISMS effectiveness
Review level of residual and acceptable risk
Conduct internal ISMS audits
Regular management review of ISMS
Record actions and events that impact on ISMS
3
4
Implement identified improvements
Take corrective or preventive action
Apply lessons learned (inc. other organizations)
Communicate results to interested parties
Ensure improvements achieve objectives

A MODEL FOR CONTINGENCY PLAN

- To help you understand the structure and use of the incident response(IR) and disaster recovery(DR) plans, this section presents a **comprehensive model** that incorporates the basics of each type of planning in a single document.

- It is not uncommon for small- to medium-sized organizations to use such a document.

- The single document supports concise planning and encourages smaller organizations to develop, test, and use IR and DR plans.

- The model presented is based on analyses of disaster recovery and incident response plans of dozens of organizations.

A MODEL FOR CONTINGENCY PLAN

The Planning Document :

The first document created for the IR and DR document set is the incident reaction document.
The key players in an organization, typically the top computing executive, systems administrators, security administrator, and a few functional area managers, get together to **develop the IR and DR plan.**

A MODEL FOR CONTINGENCY PLAN

These are the six steps in the consolidated contingency planning process :

- ✓ Identifying the mission- or business-critical functions: The organization identifies those areas of operation that must continue in a **disaster to enable the organization to operate**. These must be prioritized from most critical to least critical **to allow optimal allocation of resources** (time, money, and personnel) in the event of a disaster.

- ✓ Identifying the resources that support the critical functions: For each critical function, the organization identifies the required resources. These resources can include people, computing capability, applications, data, , services, physical infrastructure, and documentation.

- ✓ Anticipating potential contingencies or disasters: The organization brainstorms potential disasters and determines what functions they would affect.

A MODEL FOR CONTINGENCY PLAN

- ✓ Selecting contingency planning strategies: The organization identifies methods of dealing with each anticipated scenario and outlines a plan to prepare for and react to the disaster. Armed with this information, the actual consolidated plan begins to take shape.
- ✓ For each incident scenario, three sets of procedures are created and documented:

- ✓ The procedures that must be performed during the incident. **These procedures are grouped and assigned to individuals.** The planning committee begins to draft a set of these function-specific procedures.

- ✓ The procedures that must be performed immediately after the incident has ceased. Again, **separate functional areas may be assigned different procedures.**

- ✓ The procedures that must be performed to prepare for the incident. These are the details of the **data backup schedules**, the disaster recovery preparation, training schedules, testing plans, copies of service agreements, and business continuity plans

A MODEL FOR CONTINGENCY PLAN

- ✓ Implementing the contingency strategies: The organization signs contracts, acquires services, and **implements backup programs that integrate the new strategy** into the organization's routine operations.

- ✓ Testing and revising the strategy: The organization periodically tests and revises the plan.

- ✓ These are the words that all contingency planners live by: plan for the worst and hope for the best.

A MODEL FOR CONTINGENCY PLAN

Figure 5-14. A contingency plan is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization and, subsequently, to restore the organization to normal modes of business operations. The discussion of contingency planning begins with an explanation of the differences among its various elements, and an examination of the points at which each element is brought into play.

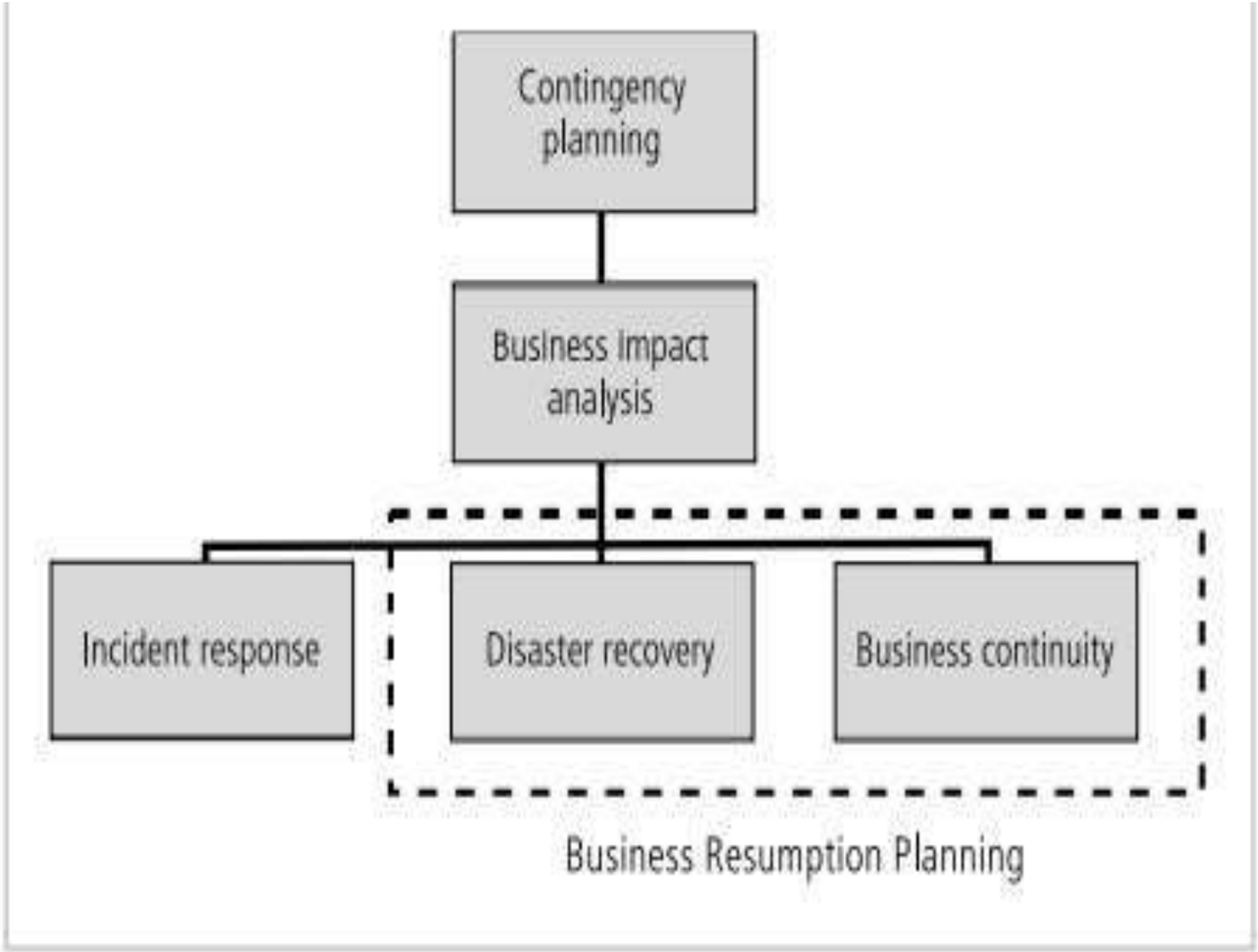


Figure 5-14 Components of Contingency Planning

A MODEL FOR CONTINGENCY PLAN

Figure 5-16. As you read the remainder of this chapter, it may help you to look back at this diagram, since many of the upcoming sections correspond to the steps depicted in the diagram.

Note that each subordinate planning task actually begins with the creation (or update) of a corresponding policy document that specifies the purpose and scope of the plan and identifies the roles and responsibilities of those responsible for the plan’s creation and implementation.

A MODEL FOR CONTINGENCY PLAN

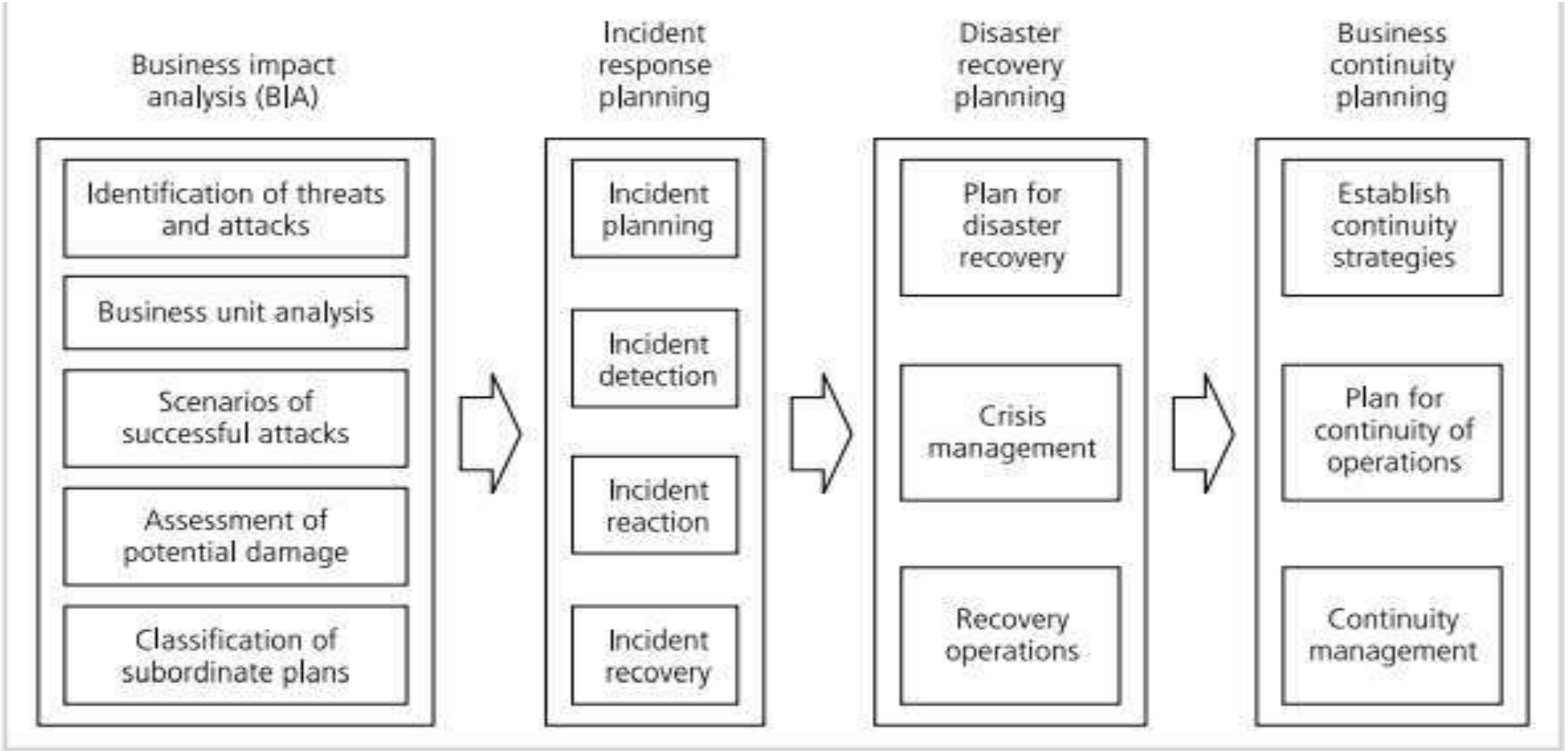


Figure 5-16 Major Steps in Contingency Planning

INTRODUCTION TO SECURITY TECHNOLOGY

Security technology encompasses various methods and tools designed to safeguard information, assets, and systems from threats. It includes physical security, network defenses like firewalls, and methods to protect remote connections.

PHYSICAL SECURITY DESIGN

Physical security involves protecting physical assets—such as buildings, servers, and critical infrastructure—from unauthorized access, theft, vandalism, and natural disasters.

Key elements include:

- **Access Control Systems**: Keycards, biometric scanners, and security personnel.
- **Surveillance Systems**: CCTV cameras, motion sensors, and alarm systems.
- **Environmental Controls**: Fire suppression systems, temperature controls for data centers.
- **Perimeter Security**: Fencing, security guards, barriers, and intrusion detection systems.

FIREWALLS AND NETWORK SECURITY

A firewall is a security mechanism that controls incoming and outgoing network traffic based on predefined rules. It serves as a barrier between trusted and untrusted networks, preventing unauthorized access. Types of firewalls include:

- **Packet-Filtering Firewalls**: Examine packets and allow or block them based on IP addresses, ports, or protocols.
- **Stateful Inspection Firewalls**: Monitor active connections and filter traffic dynamically.
- **Proxy Firewalls**: Act as intermediaries between users and services, inspecting data before forwarding.
- **Next-Generation Firewalls (NGFWs)**: Combine traditional firewalls with advanced features such as deep packet inspection and intrusion prevention.

Protecting Remote Connections

With the rise of remote work and cloud-based services, securing remote connections is critical. Some essential security measures include:

•**Virtual Private Networks (VPNs)**: Encrypt internet traffic, ensuring safe data transmission over unsecured networks.

•**Multi-Factor Authentication (MFA)**: Requires additional verification beyond passwords, such as biometrics or authentication codes.

•**Secure Socket Layer (SSL)/Transport Layer Security (TLS)**: Encrypts data for secure web browsing and online transactions.

•**Endpoint Security Solutions**: Protect remote devices with antivirus software, firewalls, and intrusion detection systems.

By integrating these security technologies, organizations can protect their assets, networks, and remote users from cyber threats and unauthorized access.

JOB ROLES IN INDUSTRY

Network Security Engineer & Security Administrator

Application Security Engineer

SUMMARY OF THE LECTURE

Introduction, **Planning for Security**

Information Security Policy, Standards, and Practices

The Information Security Blueprint,

Contingency plan and a model for contingency plan.

DISCUSSION


discussion
students
group
questions
class
time
person
participants
conversation
comment
people
minutes
think
one
Discussion
way
question
know
tolerance
comments
groups
critical
different
detectives
ideas
new
another
responses
good
made
talk
might
specific
make
just
learning
storyteller
practice
contributions
newsprint
others
Students
someone
power
also
ask
room
around
possible
team
work
give
first
get
two
view
Marcuse
allowed
large
quote
like
feel
really
see
rule
John
use
White
words
written
Learning
circle
DISCUSSION
small
things
course
much
thinking
speak
something
important
next
assumptions
point
want
asked
help
student
repressive
idea
perspective
week
best
alternative
participation
whole
right
talking
back
mean
sheet
least
interpretations
station
open
process
three
write
choose
voice
need
Make
Critical
One
wish
members
start
end
already
arguments
take
New
life