2022 | 2023

Network and Information Systems Security

Information Security Planning

Carlos Serrão
carlos.serrao@iscte-iul.pt

INSTITUTO UNIVERSITÁRIO DE LISBOA

Introduction

Information Security Planning

- An organisation's **information security effort** is **only successful** when it works **in conjunction** with the organisation's **information security policy**.
- An **Information Security Program starts** with **policy**, **standards** and **practices**, which are the **basis** for **information security architecture** and **design**.
- **Creating** and **maintaining** these elements **requires coordinated planning**.
- All organisations, do **some planning**: **strategic planning** to **manage resource allocation** and **contingency planning** to **prepare for the uncertainties** of the business environment.

Information Security Program – 10 Steps

Information Security Planning

- Establish Information Security Teams
- Manage Information Assets
- Define Regulatory Compliance and Standards
- Assess Threats, Vulnerabilities and Risks
- Manage Risks
- Create and Incident Management and Disaster Recovery Plan
- Manage Third Parties
- Implement Security Controls
- Conduct Training
- Conduct Audits

Strategic/Tactical/Operational Planning

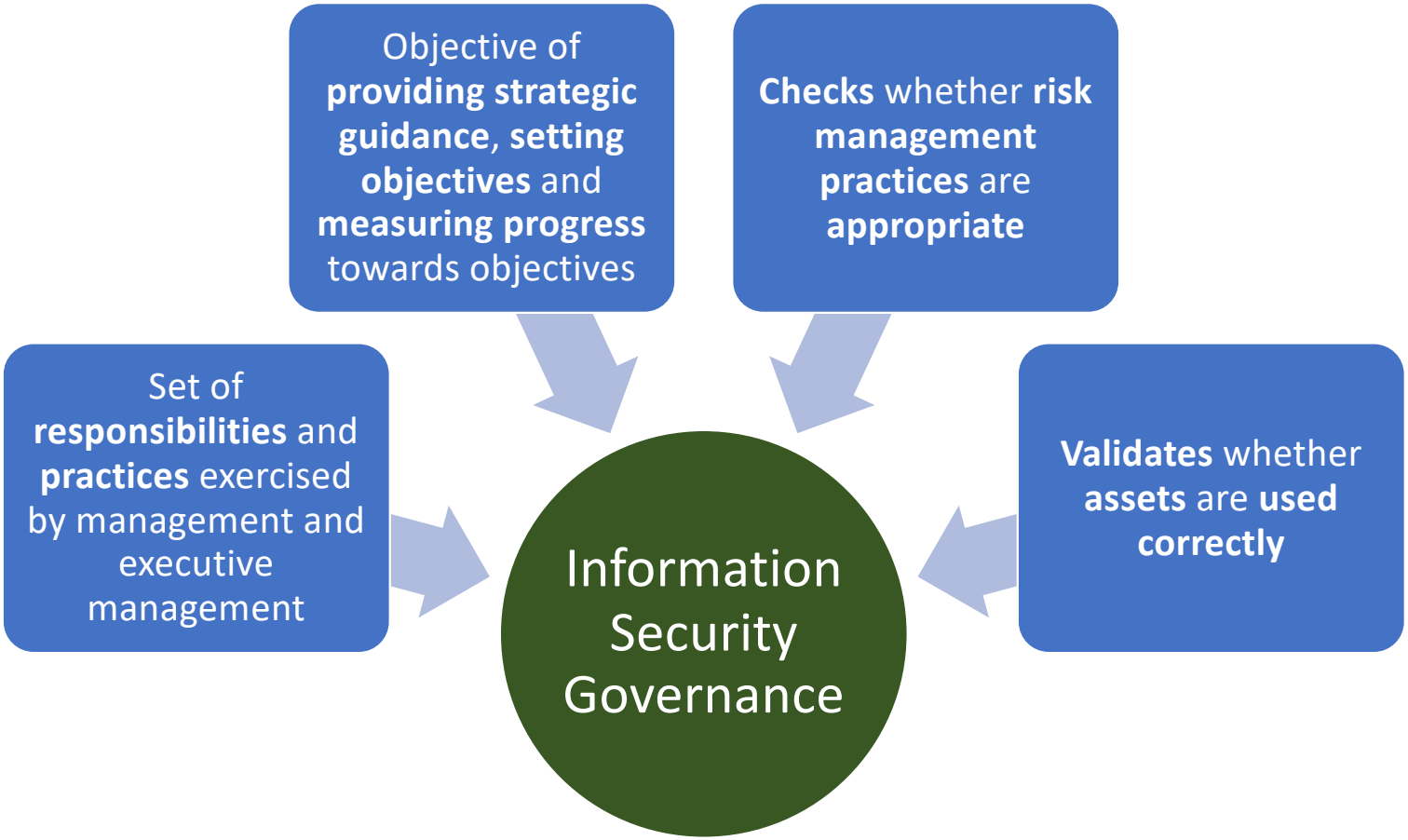
Information Security Planning

- **Strategic Plans** - long term planning, futuristic vision
  - The mission for the organisation with a 3, 5 or 10 year vision
  - Defines the long-term direction to be taken by the organisation and each of its components.
  - It should guide organisational efforts and concentrate resources on specific and clearly defined objectives.
  - To execute this strategy, the executive team must first define individual responsibilities (C-Level: CEO, COO, CFO, CIO, etc).
- **Tactical Plans** - medium-term planning and vision
  - Guided by the implementation of the strategic plans
  - Vision up to 12/24 months
  - Tactical objectives: move towards specific, measurable, achievable, relevant and time-bound (SMART) objectives.
  - The Chief Information Security Officer (CISO) and security managers use the tactical plan to organise, prioritise and acquire the necessary resources for key projects and to support the overall strategic plan.

- **Operational Plans** - short term
  - Derived from tactical planning to organise the continuous, day-to-day execution of tasks.

Information Security Governance

Information Security Planning



Information security governance is defined as "a subset of enterprise governance that **provides strategic direction**, **ensures that objectives are achieved**, **manages risk appropriately**, **uses organizational resources responsibly**, and **monitors the success or failure of the enterprise security program**," according to the Information Systems Audit and Control Association.

Information Security Governance

Need for Information Security Governance

- An **information security governance** framework helps you **prepare for risks or events before they occur** by forcing you to **continually reevaluate critical IT and business functions** through:
  - Integrated risk management functions
  - Threat and vulnerability analysis
  - Data governance and threat protection
  - Aligning business strategy with IT strategy

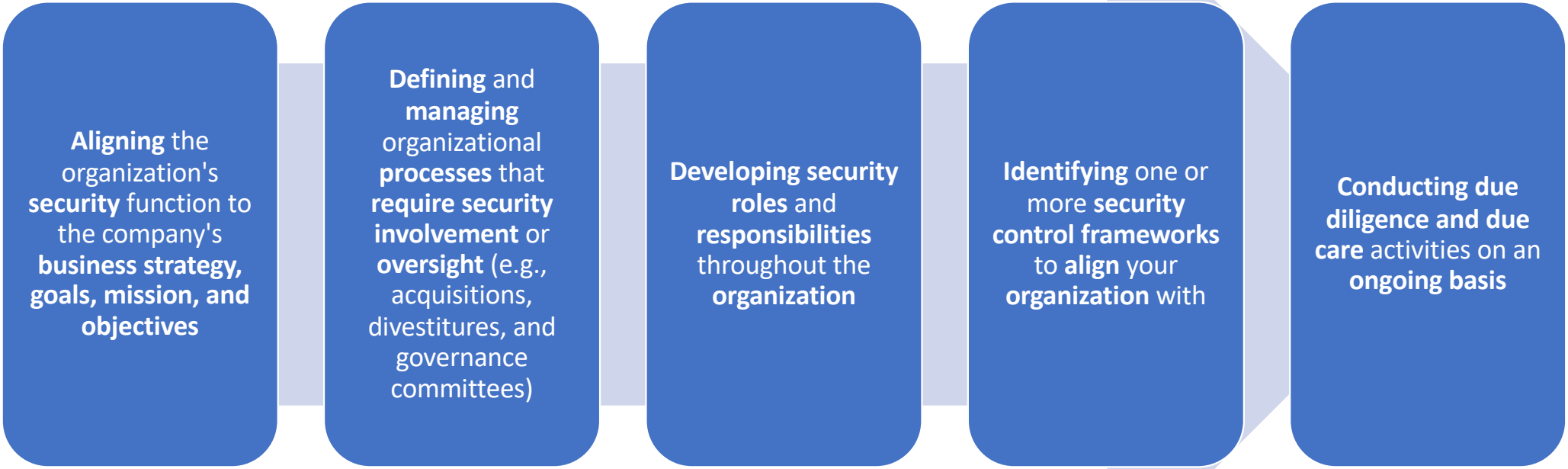
Reactive vs Proactive

- **Information security governance** also **helps** an organization move from a **reactive approach** to cybersecurity to a **proactive approach**. It allows you to:
  - **Categorize** and **mitigate risks** and **threats**
  - **Prepare** an organization for **identifying**, **remediating**, and **recovering** from a **cyberattack** or **breach**
  - **Provide** a **method** for **executive leadership** to understand their **risk posture and maturity levels**
  - Outline a **risk-based approach to the people**, **systems**, and **technology** that are used every day

Information Security Governance

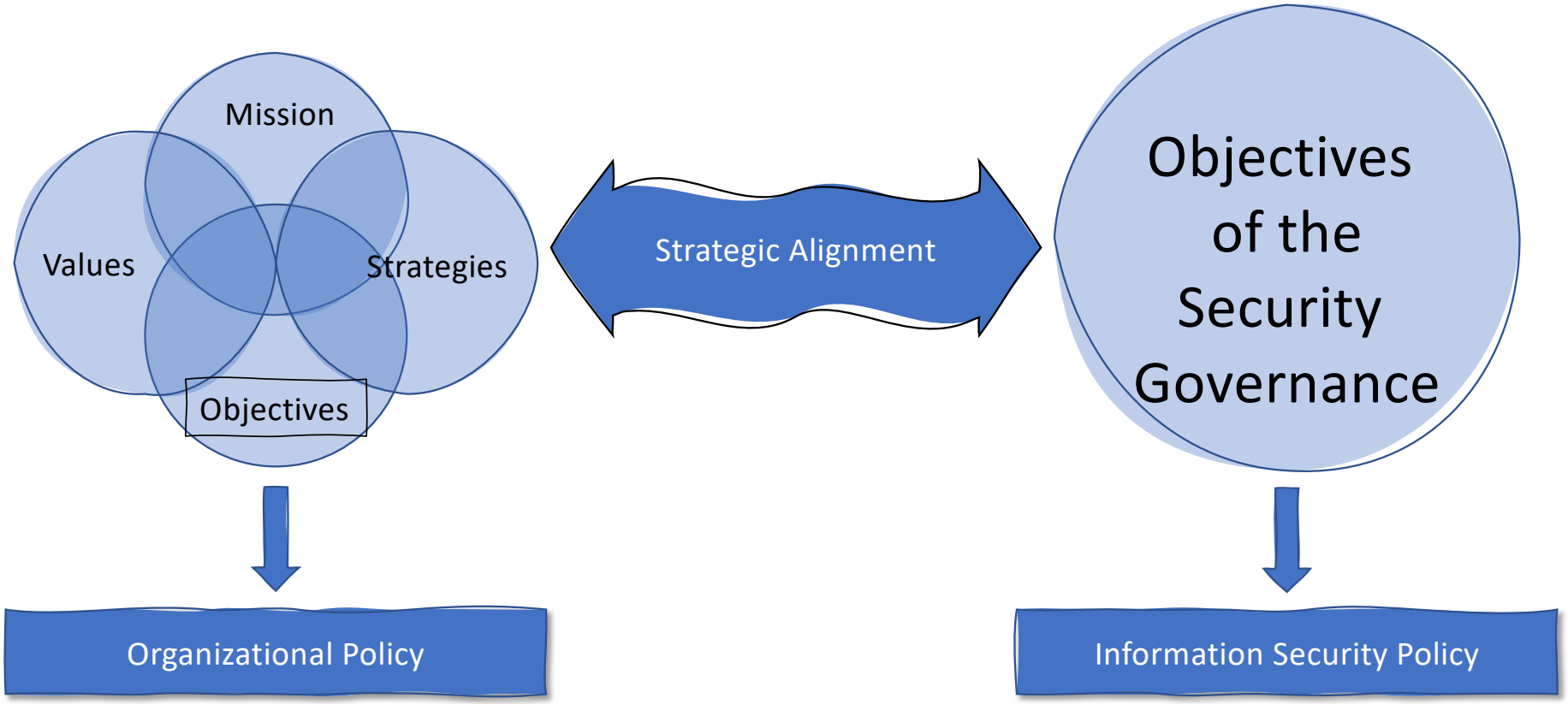
Information Security Governance Objectives

Information Security Governance Objectives

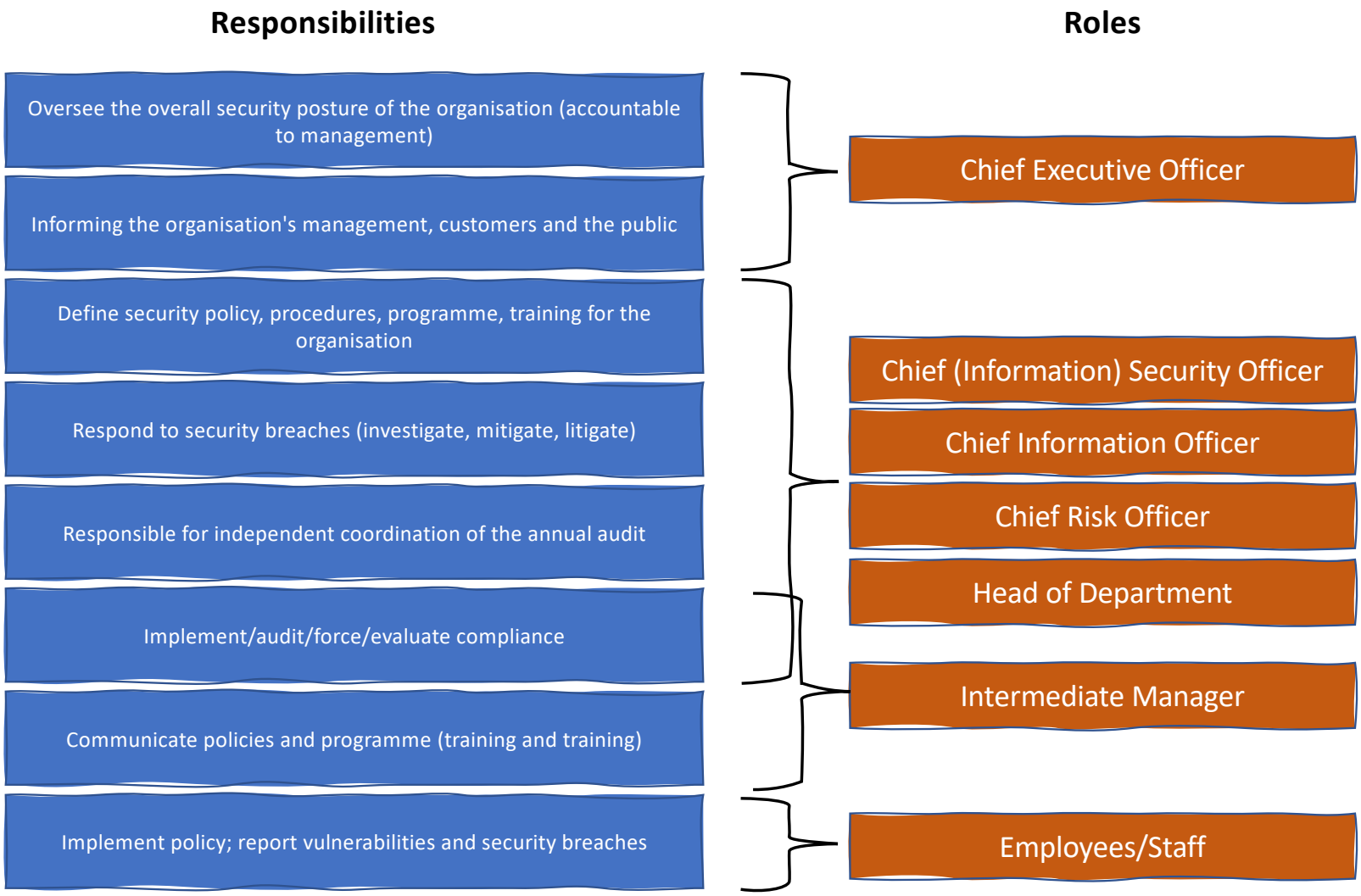


Information Security Governance

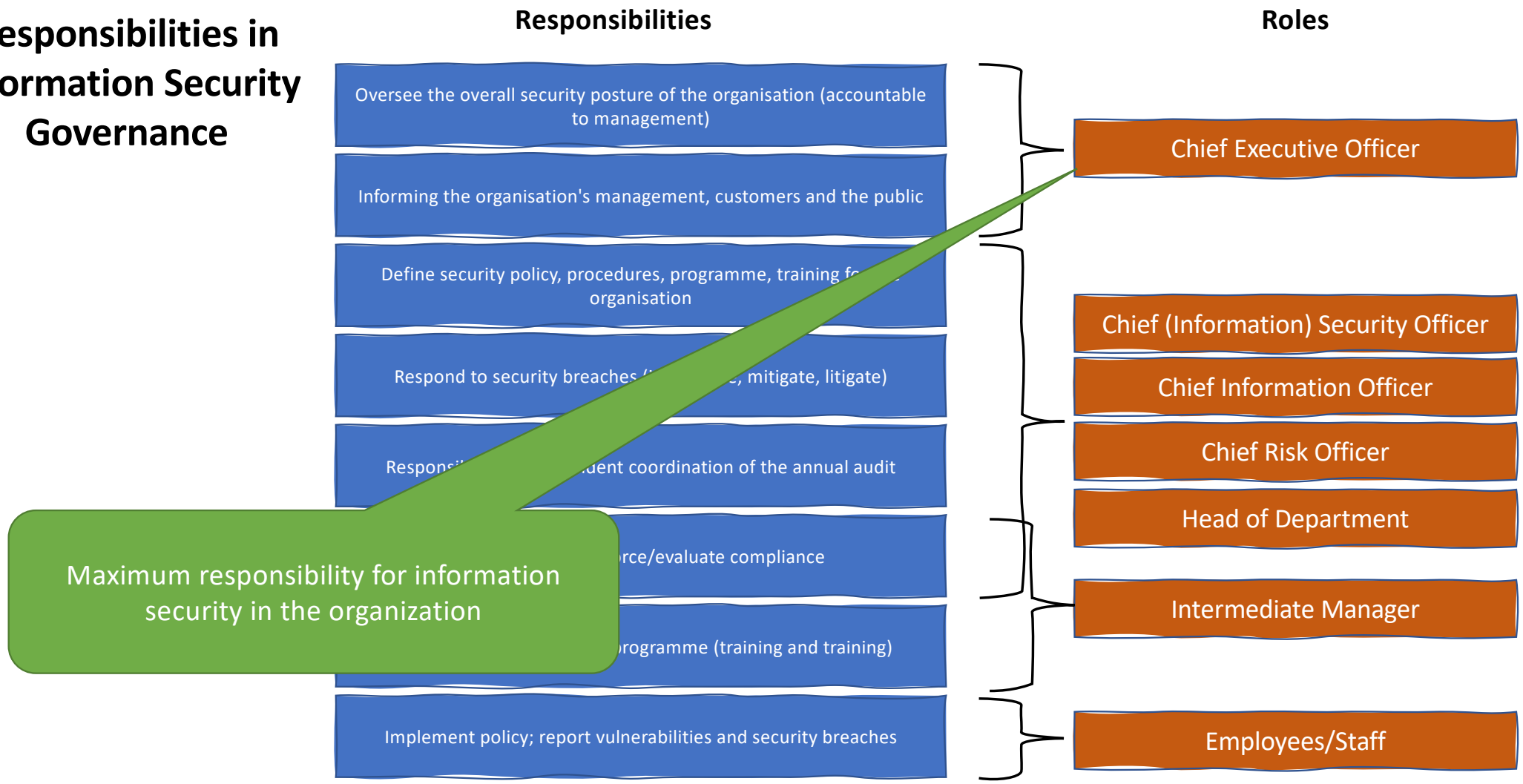
Strategic Alignment



Roles and Responsibilities in Information Security Governance



Roles and Responsibilities in Information Security Governance



Chief Information Security Officer (CISO)

Roles and priorities

The **first priority** of the **CISO** and the **information security management team** is to set up a **strategic plan** for **achieving the organisation's information security objectives**.

The **plan** is an **evolutionary statement** of how CISO and various elements of the organization **will implement the information security objectives**, which is expressed in the **Enterprise Information Security Policy** (EISP).

Chief Information Security Officer (CISO)

More roles

Chief Information Security Officer (CISO)	A CISO is the senior-level executive within an organization who is responsible for the overall management and supervision of the information security program.
Chief security officer (CSO)	A CSO is a senior-level executive within an organization who is generally responsible for all physical security and personnel security matters.
Security analyst	A security analyst is someone with technical expertise in one or more security domains who executes the day-to-day security work.
Manager or program manager	In security, a manager (or program manager) is someone who owns one or more processes related to information security.
Director	In security, a director is generally a manager of managers who is responsible for the overall strategic guidance of a group of security programs

Chief Information Security Officer (CISO)

More roles

End-User

Includes any person who accesses or handles an organization's information systems or data. Users may include full-time and part-time employees, interns, contractors, consultants, vendors, partners, and so on.

Responsibilities

- Understand, agree to, and adhere to all information security policies, procedures, standards, and guidelines, as well as any relevant regulatory and compliance requirements.
- Satisfy contractual obligations (such as nondisclosure agreements) that affect the confidentiality of the company's information and processes.
- Complete all required information security training and awareness activities by their required completion dates.
- Report any actual or suspected security violations or breaches to appropriate personnel in a timely manner.

Information Security Policy, Standards, and Practices

Information Security Planning

- The **management of the various communities of interest** (employees, information technology and information security) should make **policies** the basis of all **planning**, **design** and **implementation** of **information security**.
- **Policies guide how issues should be addressed** and **technologies used**.
- **Policies** should **never contradict the law**, must be **able to appear in court**, and should be **properly administered**.
- **Security policies** are the **least expensive controls to implement**, but **more difficult to implement properly**.

Information Securi…ces

Information Security Planning

Information security is primarily a management problem (not a technical problem) and policy is a management tool that forces people to function in a way that preserves the security of information assets.

---→The **manageme**…nology and information secur… …itation of **information securit**…

---→**Poli**…

---→**Policies** …nd should be **properly administered**.

---→**Securit**… but **more difficult to implement**

Policy as the Foundation for Planning

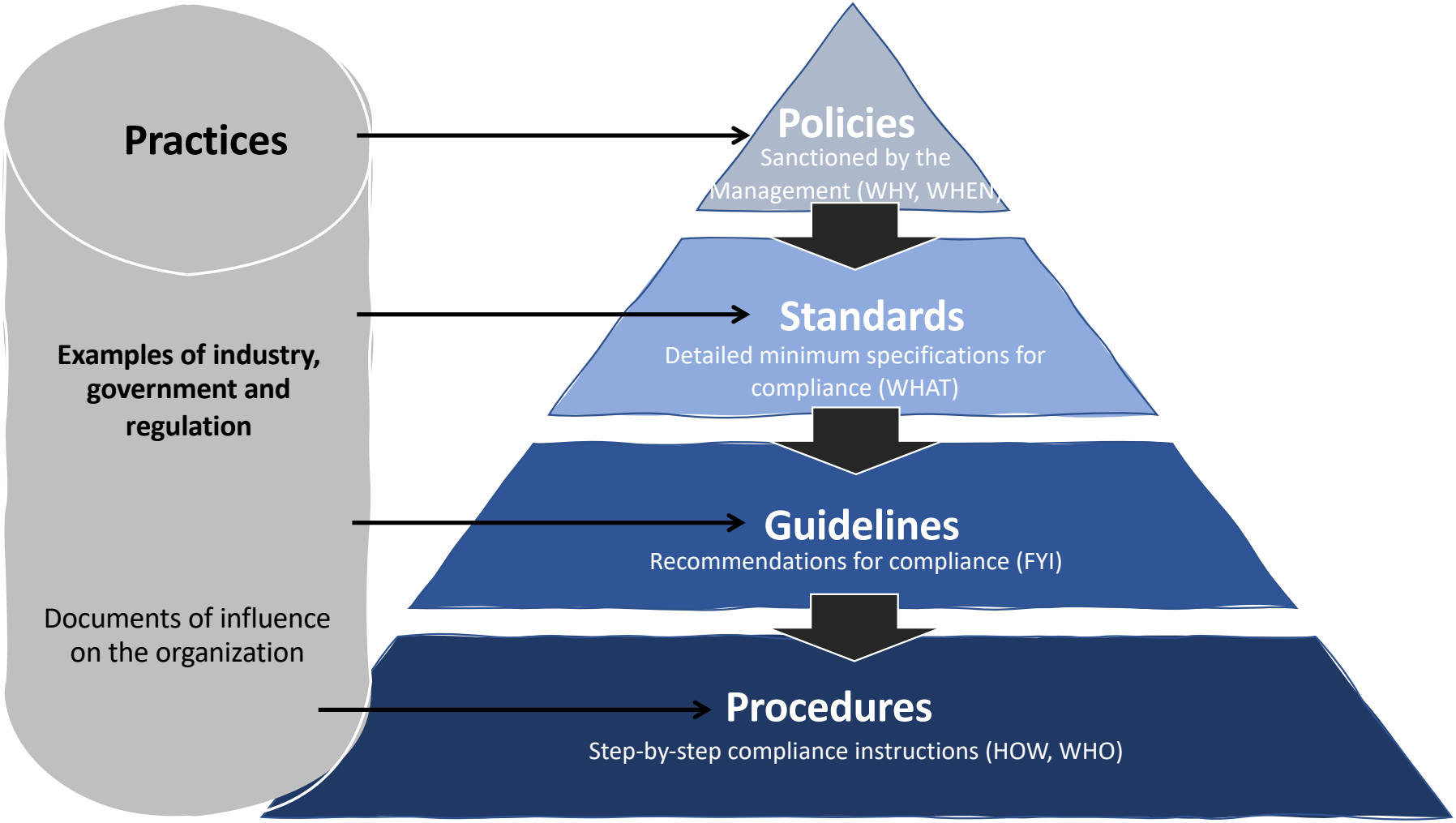
⇢**Policies** functions as an **organizational law** that **dictates acceptable** and **unacceptable behavior**.

⇢**Standards**: **more detailed statements** on what **needs to be done to comply with the policy**

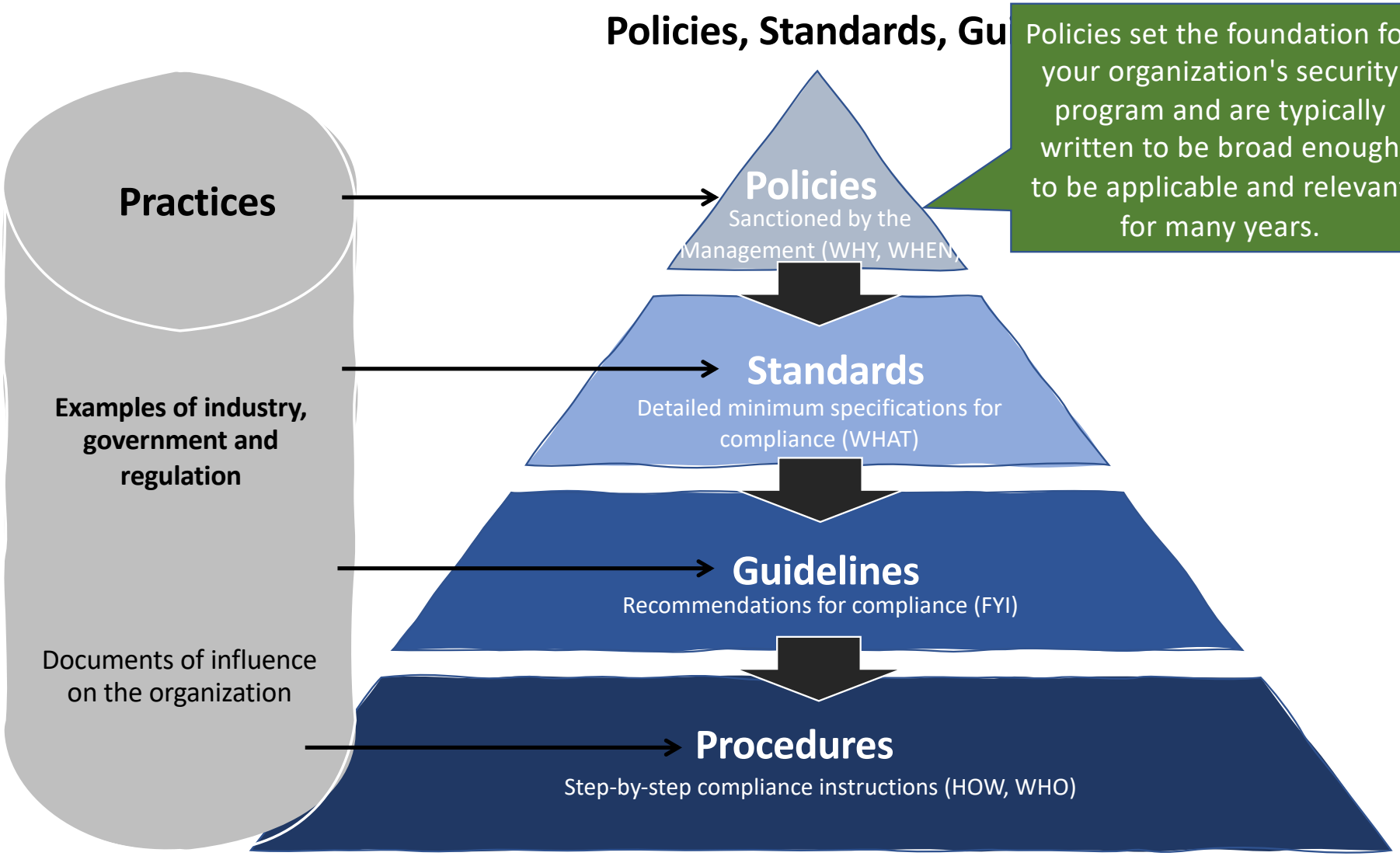
⇢**Practices**, **procedures** and **guidelines** effectively **explain how to comply with the policy**.

⇢For a policy **to be effective**, it must be properly **disseminated**, **read**, **understood** and **agreed upon** by all **members of the organisation**, and **uniformly enforced**.

Policies, Standards, Guidelines and Procedures

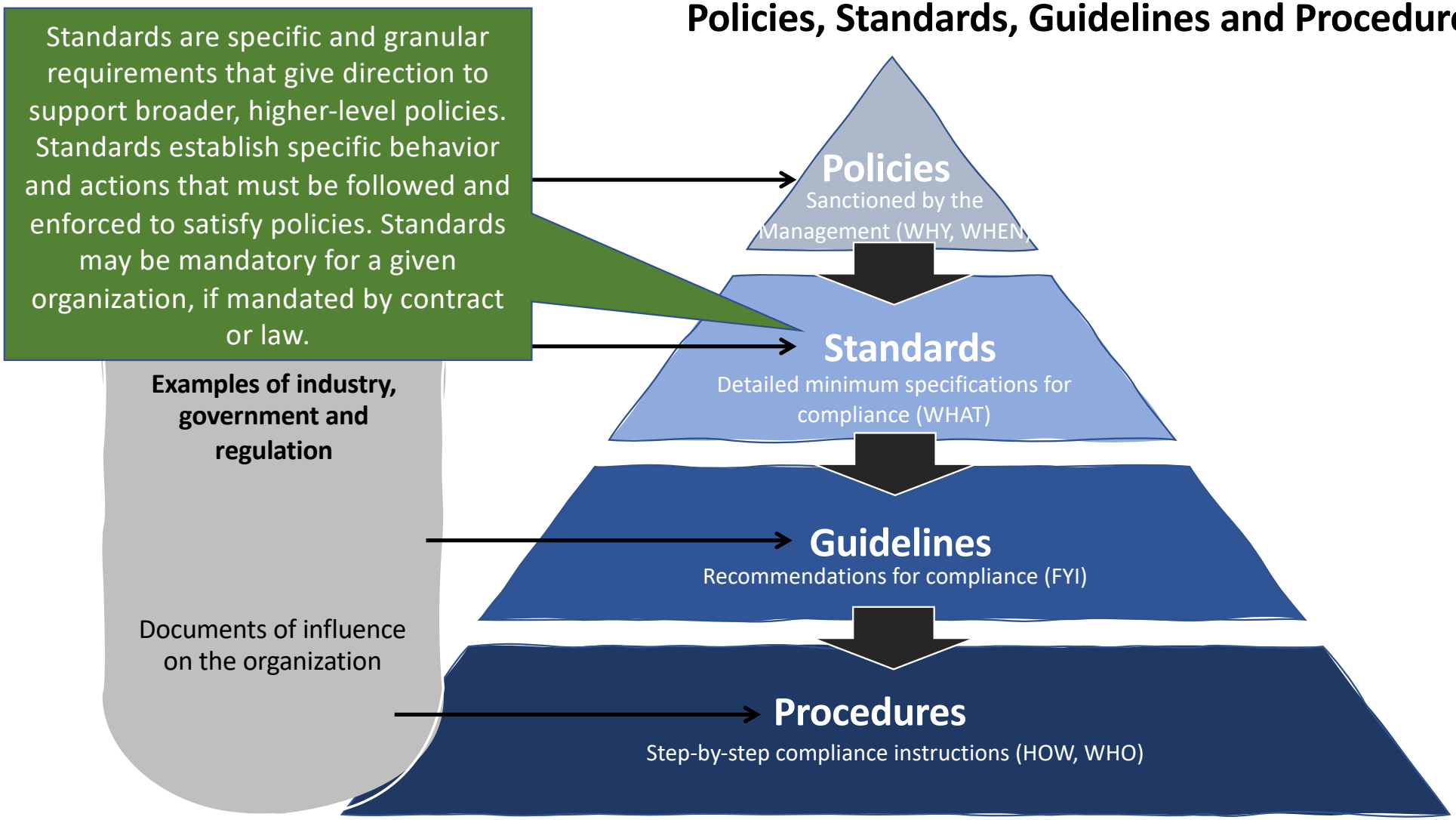


Policies, Standards, Gu

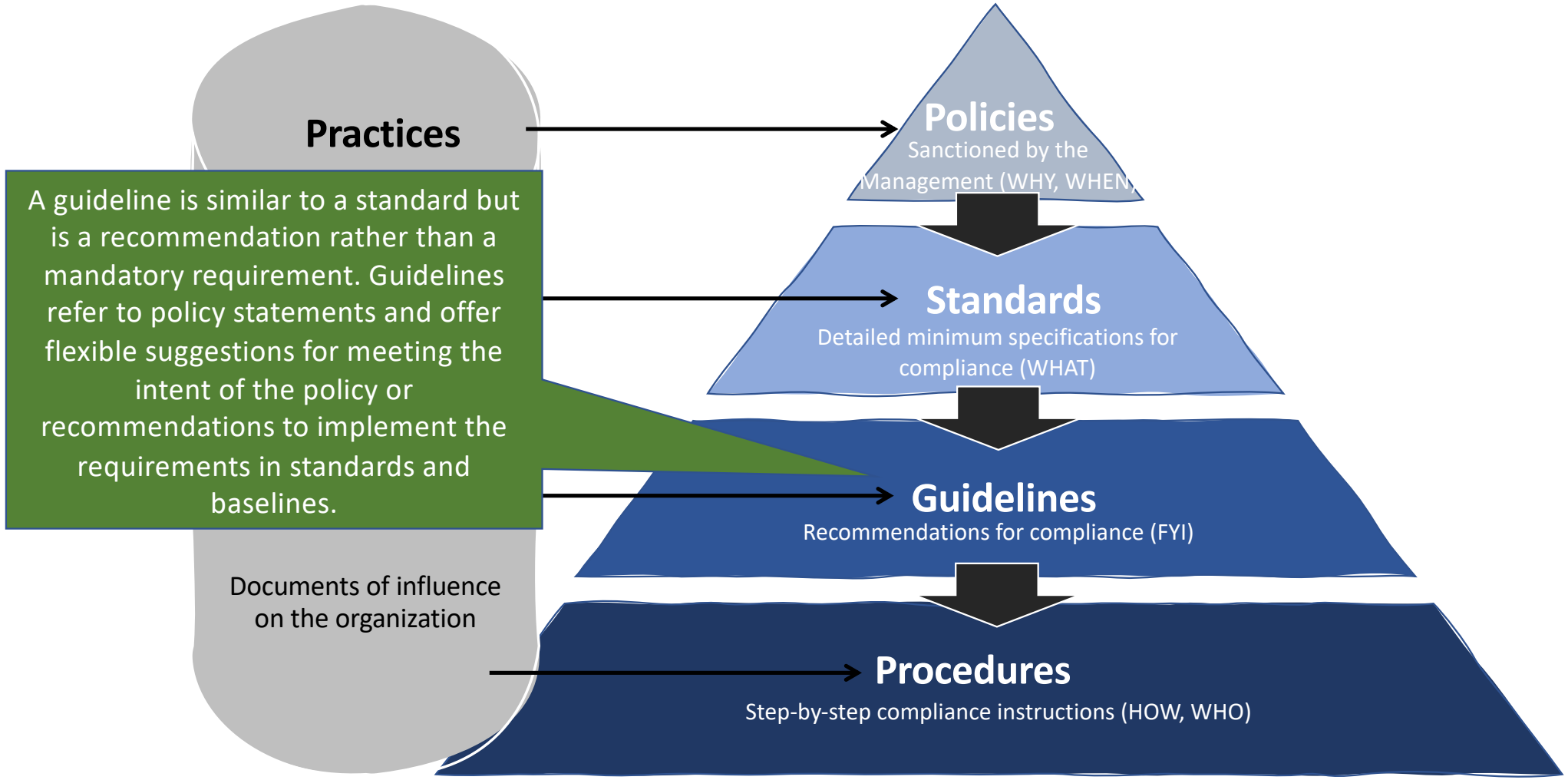


Policies, Standards, Guidelines and Procedures

Standards are specific and granular requirements that give direction to support broader, higher-level policies. Standards establish specific behavior and actions that must be followed and enforced to satisfy policies. Standards may be mandatory for a given organization, if mandated by contract or law.



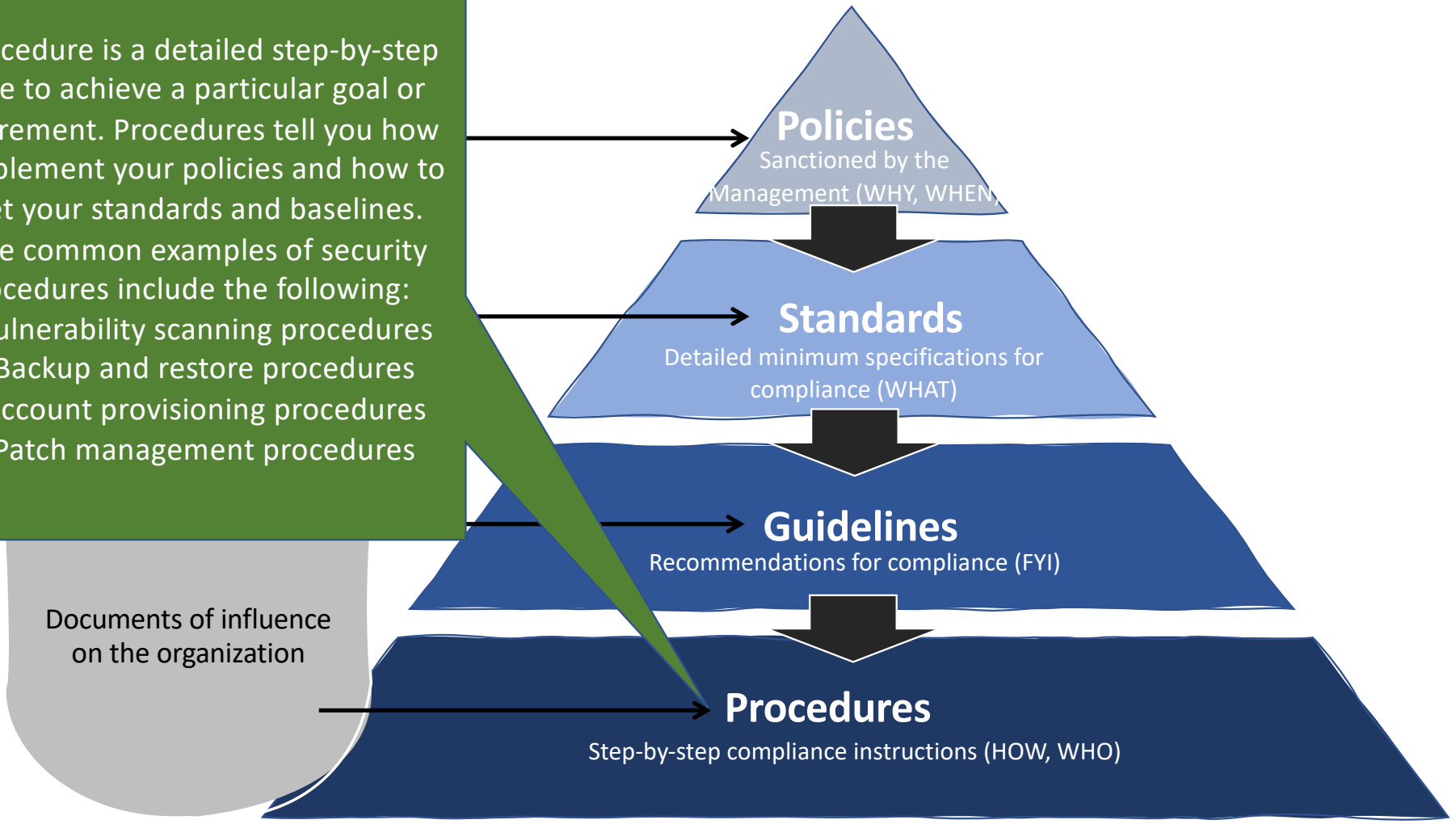
Policies, Standards, Guidelines and Procedures



Policies, Standards, Guidelines and Procedures

A procedure is a detailed step-by-step guide to achieve a particular goal or requirement. Procedures tell you how to implement your policies and how to meet your standards and baselines. Some common examples of security procedures include the following:

- Vulnerability scanning procedures
- Backup and restore procedures
- Account provisioning procedures
- Patch management procedures



Policy as the Foundation for Planning

- According to **NIST SP 800-12 rev 1** management **must define three types of security policies**:
  - Enterprise Information Security Policy [a.k.a. Information Security Policy] (EISP)
  - Issue-Specific Security Policy (ISSP)
  - System-Specific Security Policy (SSSP)

Enterprise Information Security Policy (EISP)

- **Defines** the **strategic direction**, **scope** and **tone** for **all security efforts** within the organization
- **Executive-level document**, usually **drafted by** or **in collaboration** with the Chief Information Officer (CIO)
- Typically **addresses compliance** in **two areas**:
  - Ensure **compliance** with the **requirements** to **establish the program** and **assign responsibilities** to the various organizational components
  - Use of **specific sanctions** and **disciplinary actions**

Enterprise Information Security Policy (EISP)

- The **elements** of the EISP **should include**:
  - **Overview** of the company's **security philosophy**
  - **Information** on the **structure of the organization** and **persons** with information security functions
  - **Responsibilities** articulated by **security** shared by **all members of the organisation**
  - **Unique security responsibilities** for **each role in the organization**

Enterprise Information Security Policy (EISP)

EISP Components

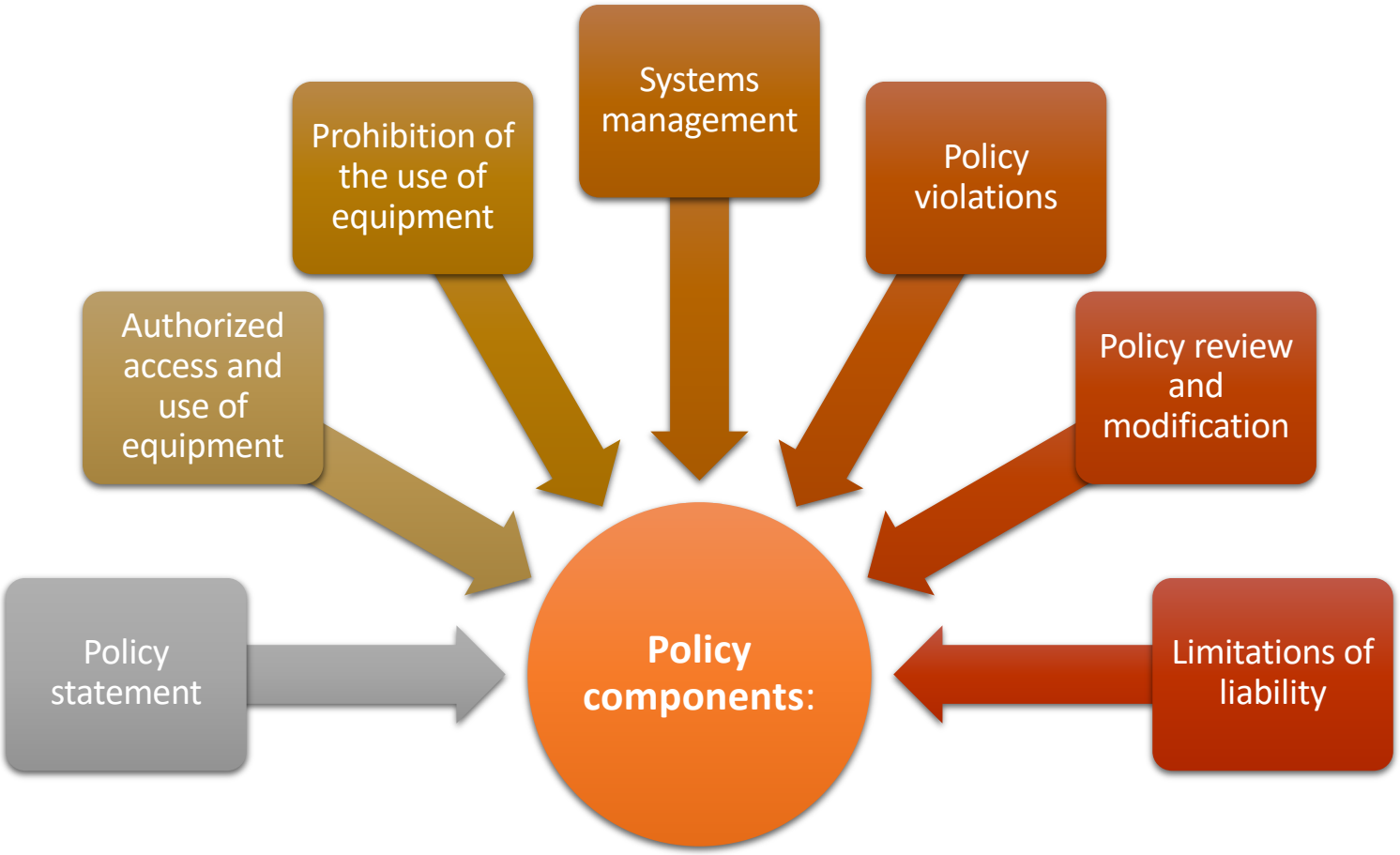
Component	Description
Goal statement	It answers the question "What is this policy for?". Provides the framework that helps the reader understand the purpose of the document. It may include text such as "This document: Identifies the elements of a good security policy Explains the need for information security Specifies the various categories of information security Identifies information security roles and responsibilities Identifies appropriate levels of safety through standards and guidelines This document sets out the objectives in terms of information security and direction for the organization. Departments should establish the standards, guidelines, and operational procedures that comply with and reference this policy when seeking to meet their specific needs."
Elements of Information Security	Defines information security. For instance: "Protect the confidentiality, integrity and availability of information during processing, transmission and storage, through the use of policy, education and training, and technology..." This section may also display security settings or philosophies that clarify the policy.
Need for Information Security	It provides information on the importance of information security in the organization and the legal and ethical obligation to protect critical information from customers, employees and markets.
Information Security Responsibilities and Roles	Define the organizational structure designed to support information security in the organization. Identifies the categories of persons responsible for information security (IT department, management, users) and their responsibilities, including the maintenance of this document.
References to other information standards or guides	Lists other standards that influence or are influenced by this policy document, including relevant laws and other policies.

Issue-Specific Security Policy (ISSP)

- The **ISSP**:
  - Addresses specific **areas of technology**
  - Requires **frequent updates**
  - Contains a **statement** on the organisation's **position on the specific issue**
- Three common approaches when creating and managing ISSP:
  - Create a series of independent ISSP documents
  - Create a single comprehensive ISSP document
  - Create a modular ISSP document

- ISSP **can address topics such as**:
  - Email
  - Internet use and WWW
  - Minimum computer settings to be defended against viruses and worms
  - Prohibitions against hacking or testing against the organization's security controls
  - Home use of company computers
  - Use of personal equipment in the company's network (BYOD)
  - Use of communication technologies
  - Use of copy equipment
  - Use of portable storage equipment (USB pens, portable discs, etc.)
  - Cloud storage usage
  - ...

Issue-Specific Security Policy (ISSP)



Issue-Specific Security Policy (ISSP)

Components of an ISSP

1. Policy statement
   a) Scope and applicability
   b) Definition of the technologies addressed
   c) Responsibilities
2. Authorized access and use of equipment
   a) User access
   b) Responsible and fair use
   c) Privacy protection
3. Prohibited use of equipment
   a) Disruptive use or misuse
   b) Criminal use
   c) Offensive or harassing materials
   d) Copyrighted, licensed or other intellectual property materials
   e) Other restrictions
4. Systems Management
   a. Management of stored materials
   b. Employee monitoring
   c. Virus protection
   d. Physical security
   e. Encryption
5. Policy violations
   a) Procedures for reporting violations
   b) Penalties for violations
6. Policy revisions and modifications
   a) Scheduled review of policy modification procedures
   b) Statement of limitations of legal liability
7. Limitations of liability
   a) Statements of responsibility
   b) Other statements of limitations of liability if necessary

System-Specific Security Policy (SSSP)

- SSSPs often function as **standards** or **procedures** used in **configuring or maintaining** systems (for example, they can describe how to configure a firewall)
- **System-specific policies** are divided **into two groups**:
  - Management guidance
  - Technical specifications
    - Access control lists (ACLs) can restrict access for a particular user, computer, time, duration - even a particular file.
    - Configuration rules policies govern how the security system reacts to incoming data.
- SSPP together **combine** management guidelines and technical specifications.

Policy management

- **Policies** should **be managed** as they **change constantly**.
- In to **remain viable**, security policies **must have**:
  - A responsible manager
  - A calendar of revisions
  - Definition of review procedures and practices
  - A date of issue and review of the policy
  - Automated policy management

The Information Security Plan

Information Security Planning

- Basis for the **design**, **selection** and **implementation** of all elements of the **security program**, including **implementation** and **management** of **policies**, **risk management** programmes, **education** and **training programmes**, **technological controls** and **program management**.
- **Detailed version** of the **security framework** (outline of the global information security strategy for the organization)
- Specifies the tasks and the order in which they should be performed
- It should also serve as a **scalable**, **up-to-date** and **comprehensive plan** for current and future information security needs

The ISO 27000 series

Information Security Planning

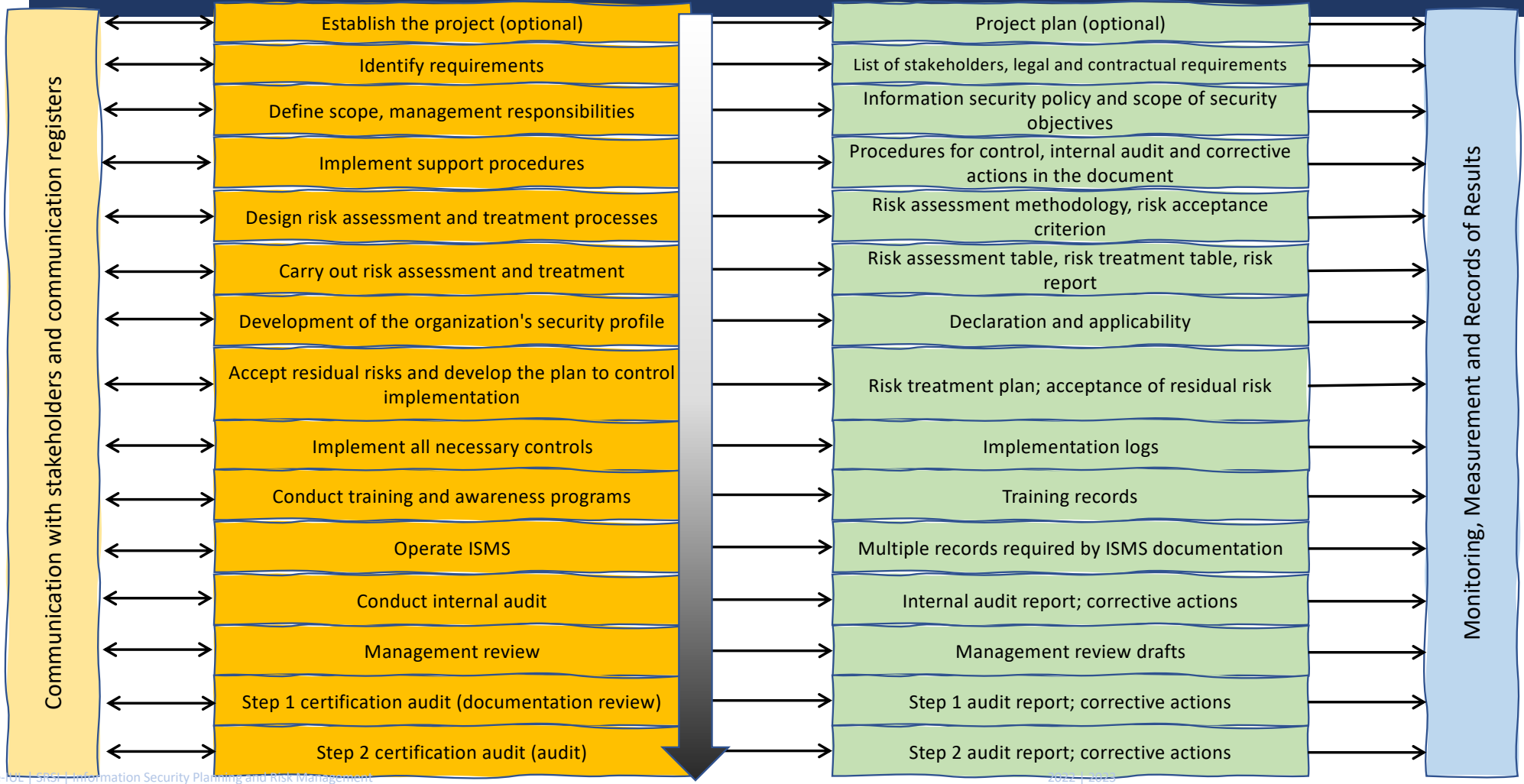
- One of the most widely referenced security models
- Standard framework for information security, which states that organizational security policy is necessary to provide management direction and support
- The aim is to provide recommendations for information security management
- Provides a starting point for the development of organizational security

Offer guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization.... The document specifically identifies itself as "a starting point for developing organization specific guidance." It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details or "how-to's."

ISO/IEC 27002:2013

ISO 27000 Series of Standards	Title or Topic	Comment
27000:2014	Series Overview and Terminology	Defines terminology and vocabulary for the standards series
27001:2013	**Information Security Management System Specification**	**Derivative of BS7799:2**
27002:2013	**Code of Practice for Information Security Management**	**Renamed ISO/IEC 17700; derived from BS7799:1**
27003:2010	**Information Security Management Systems Implementation Guidelines**	**Indications for planning project requirements for the implementation of an ISMS**
27004:2009	Information Security Measurements and Metrics	Metrics and performance measures of information security management decisions
27005:2011	**ISMS Risk Management**	**Supports 27001, but does not recommend any specific method of risk management**
27006:2011	Requirements for Bodies Providing Audit and Certification of an ISMS	Serves to support the accreditation of ISMS certification entities
20007:2011	Guideline for ISMS Auditing	Focuses on management systems
27008:2011	Guideline for Information Security Auditing	Focuses on security checks
27013:2012	Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001	Supports the implementation of integrated dual management system.
27014:2013	**Information Security Governance Framework**	**ISO approach to security governance.**
27015:2012	Information Security Management Guidelines for Financial Services	Guide for financial services organizations.
27019:2013	Information security management guidelines for process controlo systems to the energy industry	Focuses on helping organizations in the energy industry implement ISO standards.

ISO/IEC 27001: 2013



ISO/IEC 27002:2013

ISO 27002:2013 Contents
Foreword
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communication security
14. System acquisition, development, and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance
Bibliography

NIST Security Models

Alternative approaches to ISO/IEC 27000

- Another possible approach described in NIST Information Security Resource Center available documents
  - SP 800-12: An Introduction to Computer Security: The NIST Handbook
  - SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
  - SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems
  - SP 800-30 Rev. 1: Guide for Conducting Risk Assessments
  - SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - SP 800-39: Managing Information Security Risk: Organization, Mission, and Informa- tion System View
  - SP 800-50: Building an Information Technology Security Awareness and Training Program
  - SP 800-55 Rev. 1: Performance Measurement Guide for Information Security
  - SP 800-100: Information Security Handbook: A Guide for Managers

NIST Cybersecurity Framework

- It consists of three fundamental components:
  - **Core:** set of information security activities that an organization is expected to carry out and its desired results
    - Identify; Protect, protect, protect: Detect; Answer; Recover
  - **Levels:** help relate the maturity of security programs and implement correspondents' measures and functions
    - Tier 1: Partial; Tier 2: Risk Informed; Tier 3: Repeatable; Tier 4: Adaptative
  - **Profile:** used to perform a gap analysis between the current state and a desired state of security/information risk management

NIST Cybersecurity Framework





IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
- Asset Management - Business Environment - Governance - Risk Assessment - Risk Management Strategy	- Awareness Control - Awareness and Training - Data security - Info Protection and Procedures - Maintenance - Protective Technology	- Anomalies and Events - Security Continuous Monitoring - Detection Process	- Response Planning - Communications - Analysis - Mitigation - Improvements	- Recovery Planning - Improvements - Communications

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework

⇢Seven-step approach to program implementation/improvement:

1. Set priorities and scope
2. Guide
3. Establish the current profile
4. Conduct risk assessment
5. Set the target profile
6. Determine, analyze, prioritize gaps
7. Implement action plan

Other Sources of Information Security Frameworks

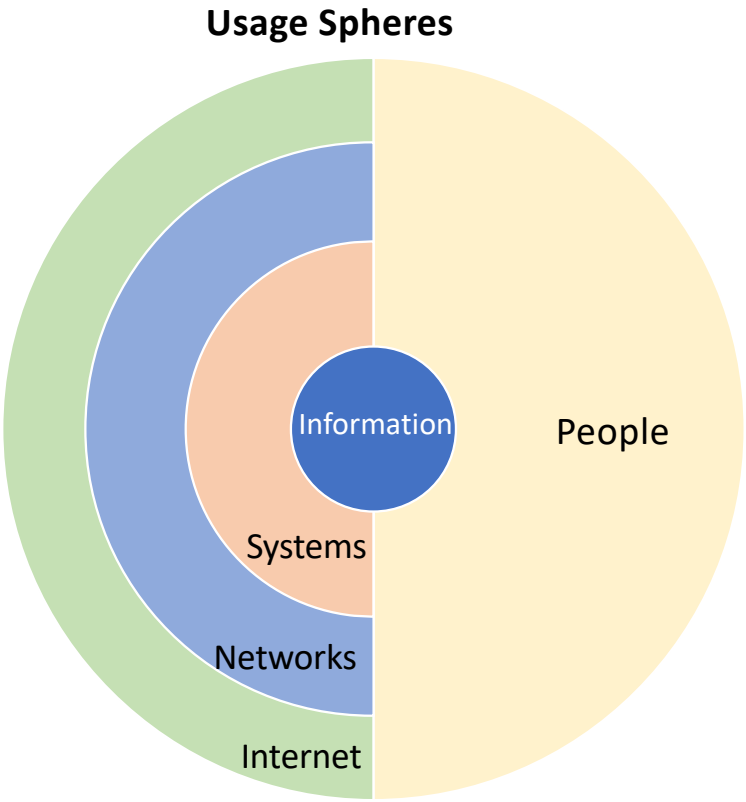
- Computer Emergency Response Team Coordination Center (CERT/CC) [www.cert.org]
- Information Security Forum [www.securityforum.org]
- Information Systems Audit and Control Association [www.isaca.org]
- International Association of Professional Security Consultants [www.iapsc.org]

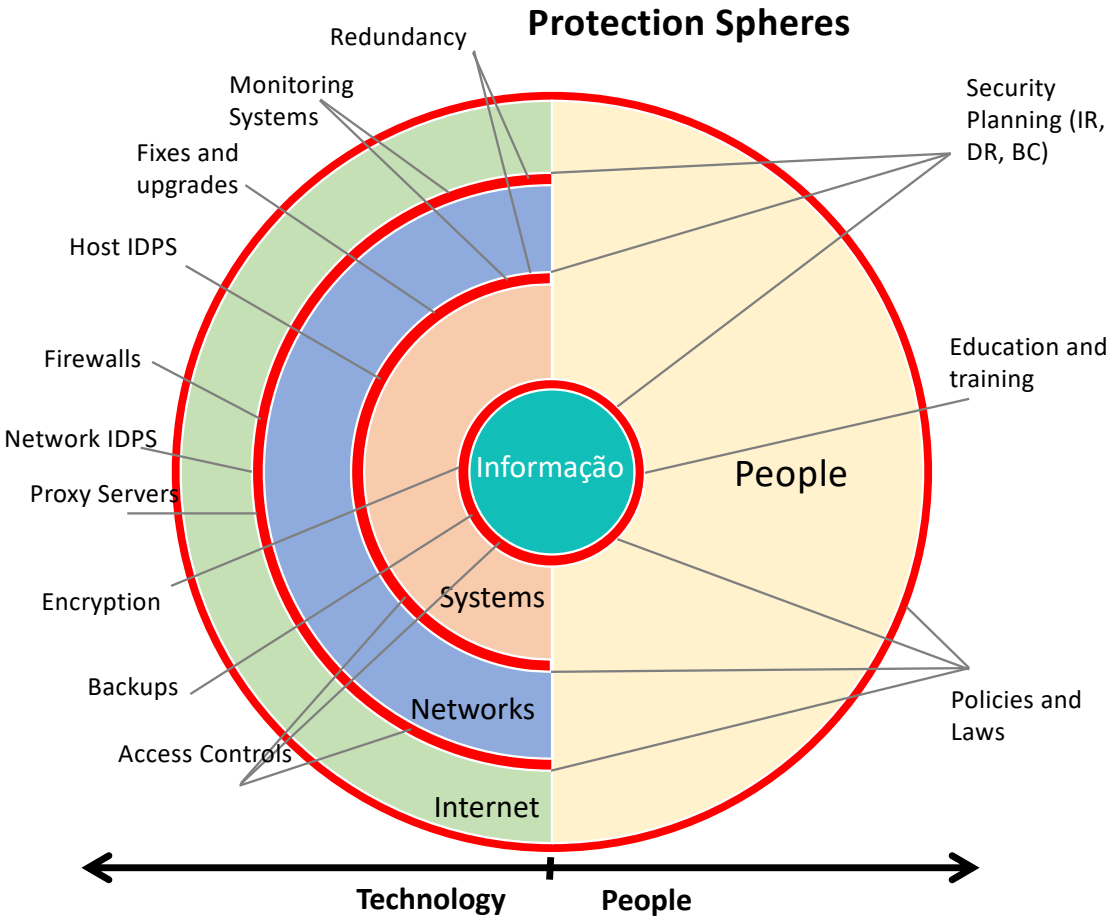
Security Architecture Design

- **Safety spheres: safety framework fundamentals**
- Control levels:
  - **Management controls** define the **direction and scope of security processes** and provide **detailed instructions for implementation**.
  - **Operational controls** are **directed to personnel and physical security**, and to the **protection of inputs/outputs of production**.
  - **Technical controls** are **tactical and technical implementations** related to the **design and integration of security** in the organisation.

Security Spheres

Security Architecture





Design of the Security Architecture

- **Defense in depth**
  - Layered security implementation
  - Requires the organisation to establish multiple levels of security checks and safeguards
- **Security perimeter**
  - Security border protecting internal systems from external threats
  - Does not protect against internal attacks from employee threats or physical threats on-premises

Security Education, Training and Awareness

⇢When the **general security policy exists**, the **Security Education, Training and Awareness (SETA)** program **should be implemented**.

⇢SETA is a **control measure designed to reduce accidental safety breaches**.

⇢The SETA programme consists of **education**, **training**, and security **awareness**.

⇢**Increases security** by **improving awareness**, **developing skills and knowledge**, and **deepening knowledge**

⇢**All members** of an organization **need to be trained and aware of information security**; **not all members need a formal diploma or certificate** in information security.

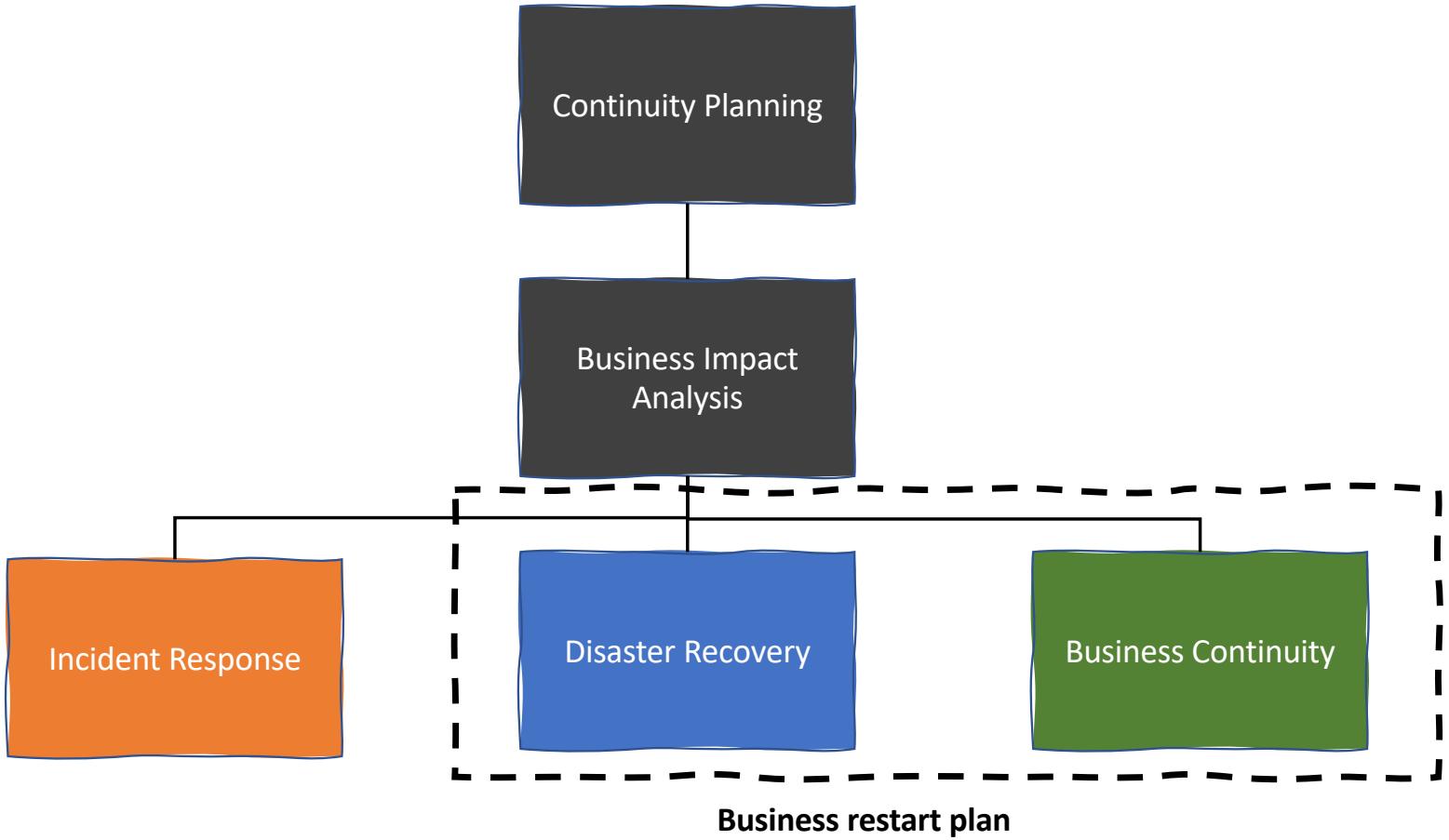
Education, Training and Awareness

	Education	Training	Awareness
Attribute	Why?	How?	What?
Level	Detailed	Knowledge	Information
Goal	Perceive	Competence	Exposure
Teaching method	Theoretical instruction: • Discussion seminars • Reading information • Applied practice	Practical instruction • Aulas • Workshop com casos de estudo • Posters	Media • Vídeos • Newsletters
Test measure	Test or work (interpreted learning)	Troubleshooting (applied learning)	• True or False • Multiple Choice
Temporal impact	In the long run	Intermediate	In the short term

Continuity Strategies

- **One of the main roles of the Management is Contingency Planning – ensuring the continuity and availability of information systems – IT MAY COMPROMISE THE BUSINESS ITSELF!!!**
  - **Incident Response Plans** (IRPs); **Disaster Recovery Plans** (DRPs); **Business Continuity Plans** (BCPs)
- Main **functions** of the above plans:
  - **IRP** focuses on **immediate response**; if the **attack intensifies or is disastrous**, the **process changes to disaster recovery** and **BCP**.
  - **DRP** typically **focuses on restoring systems** after disaster hits; as such, is **closely associated** with **BCP**.
  - **BCP** occurs **concomitantly** with **DRP** when **damage is important or continuous**, requiring **more than simply restoring information and information resources**.

Contingency Planning Components

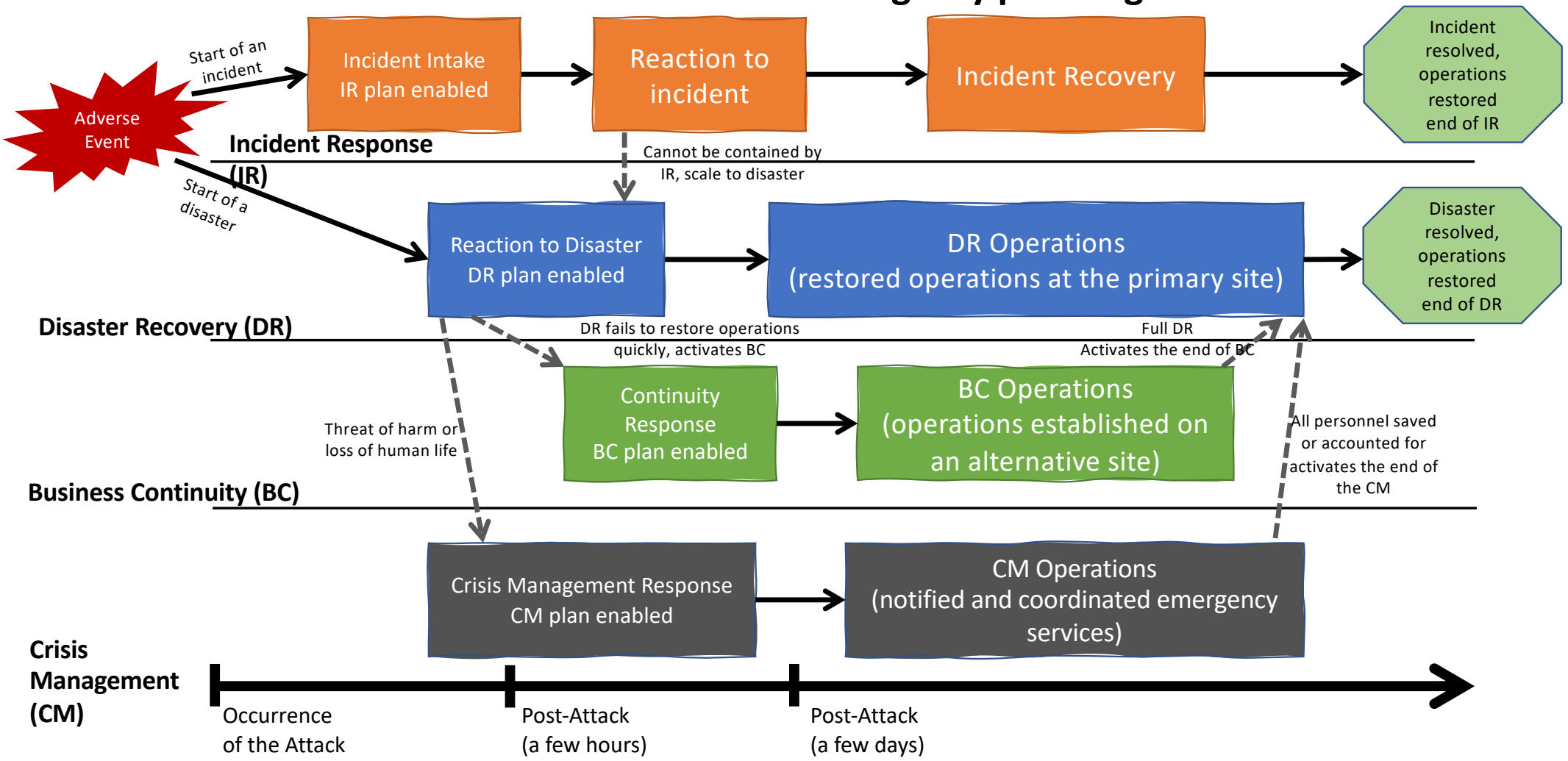


Contingency Planning Process (PC)

Contingency Planning Management Team

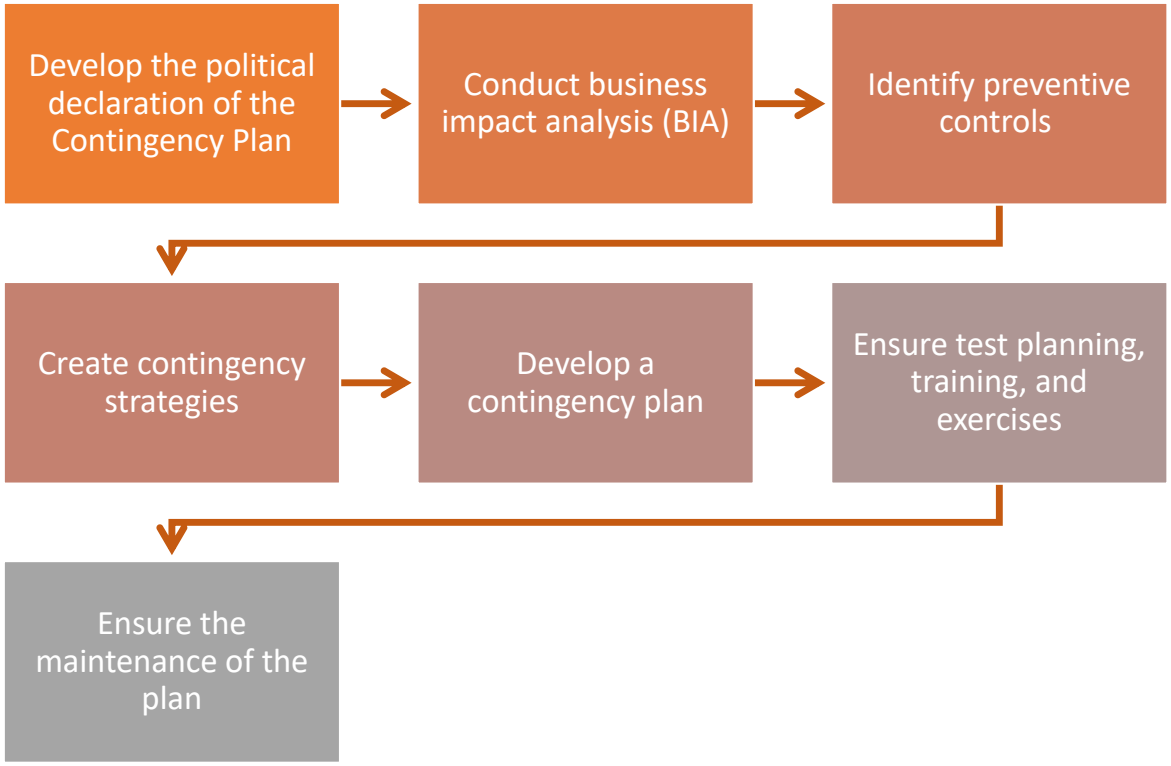
- Before planning can really begin, a team has to start the process.
  - ***Champion:*** high-level manager to support, promote and endorse project results
  - **Project manager**: leads the project and ensures the use of a good planning process, a complete and useful project plan is developed, and project resources are managed prudently
  - **Team members**: should be managers, or their representatives, from various communities of interest: business, IT and information security

Contingency planning timeline

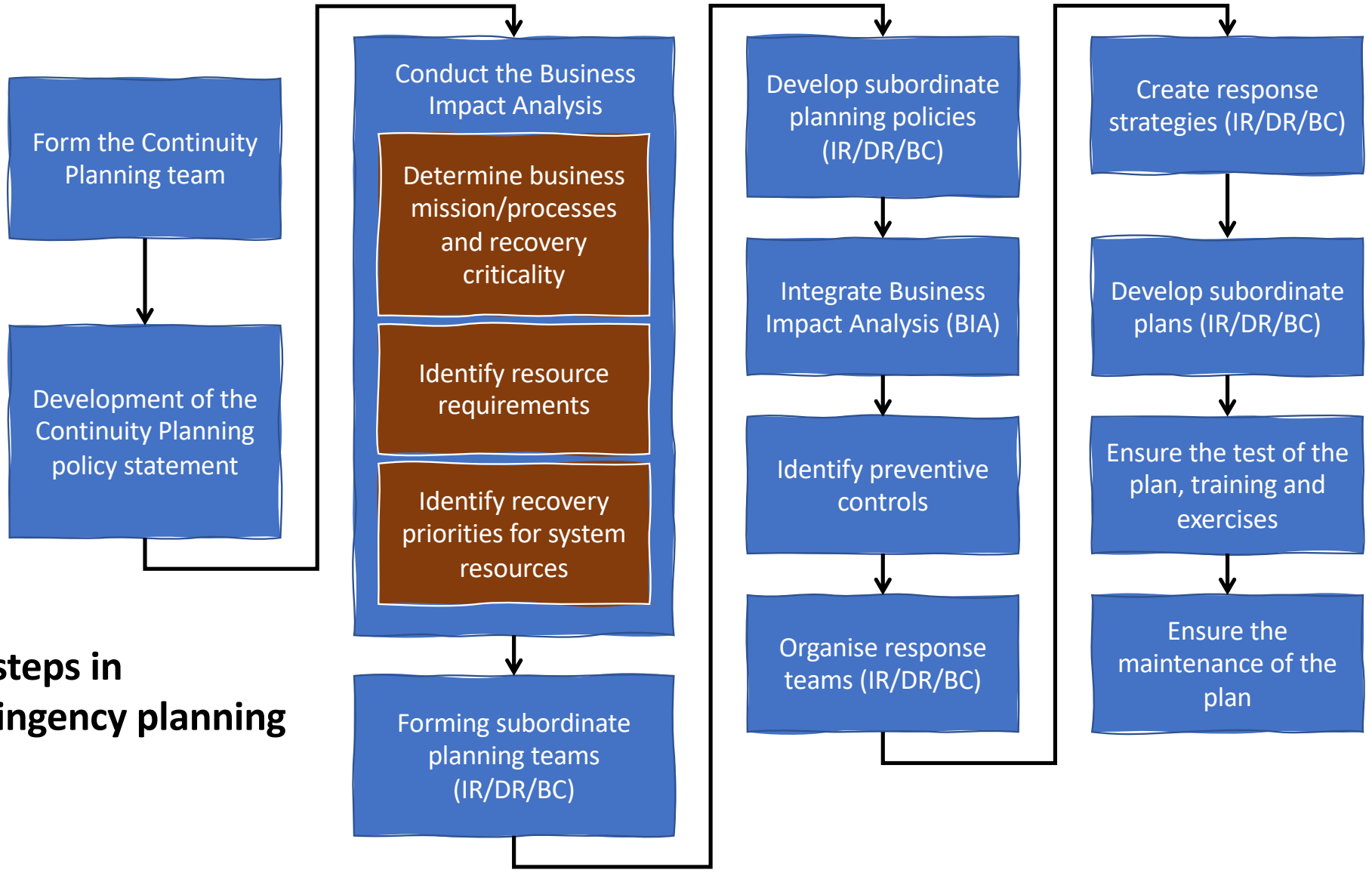


Contingency Planning Process (PC)

⇢Includes the following steps:



Key steps in contingency planning



Contingency Plan Policy

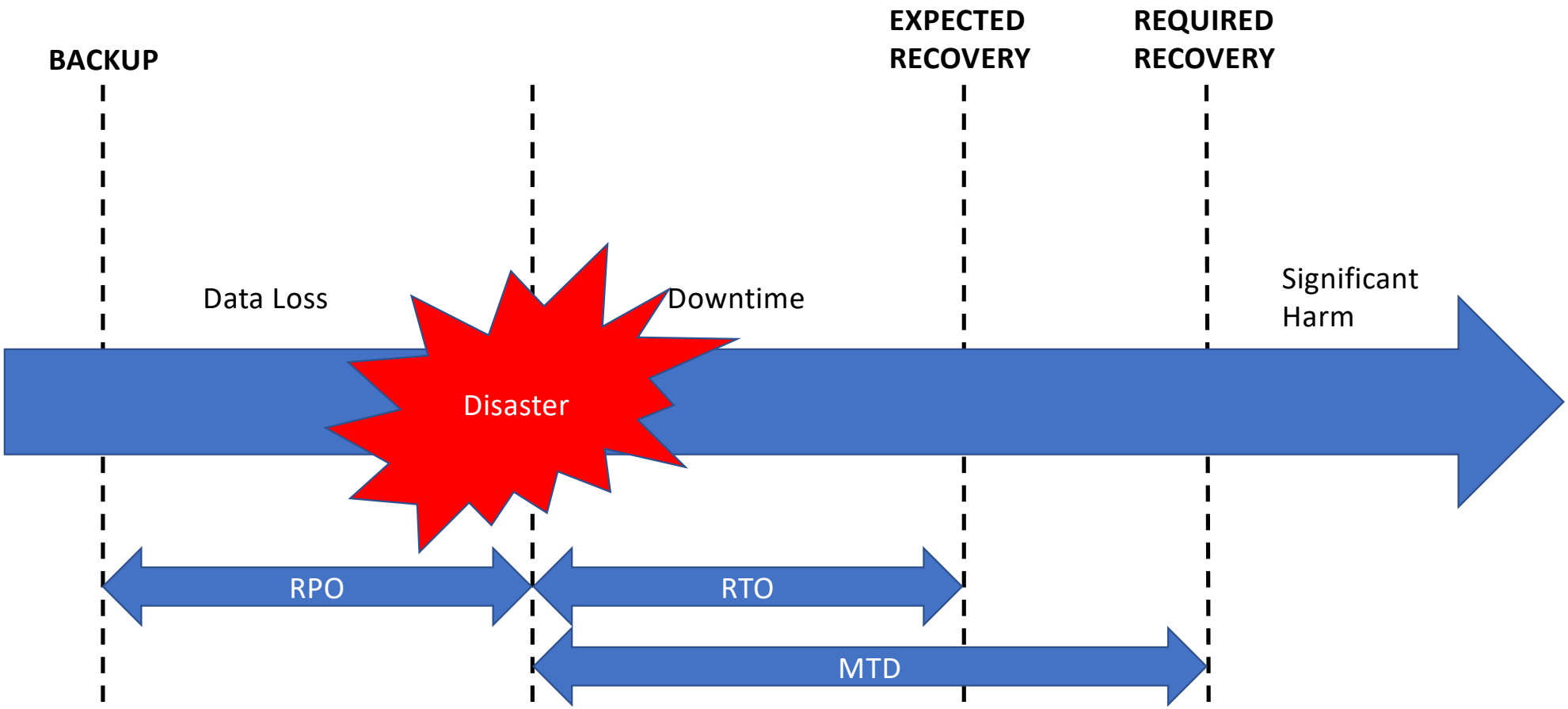
- It should contain **the following sections**:
  - Introductory statement of philosophical perspective
  - Scope/objective statement
  - Request for periodic risk assessment/BIA
  - Specification of the main pc components
  - Call/guidance in selecting recovery options
  - Obligation to regularly test the various plans
  - Identification of key regulations and standards
  - Identification of key persons responsible for PC operations
  - Challenge to members of the organization to support
  - Administrative information

Business Impact Analysis (BIA)

- Investigation and evaluation of **various adverse events** that may **affect the organisation**
- It assumes that **security checks** have been **circumvented**, **failed**, or proved **ineffective**, and that the **attack was successful**
- **Three** phases:
  - Determine **mission**/**business** processes and **recovery criticality**
  - Identify system resource **recovery priorities**
  - Identify **resource needs**
- **Important** measures:
  - **Maximum tolerable downtime** (MTD)
  - **Recovery time objective** (RTO): RTO expresses the **maximum time allowed to recover the function**. Many less formal recovery plans ignore the RTO. Time can be a critical factor, and specifying recovery time requirements helps determine the best recovery options.
  - **Recovery point objective** (RPO): Measured in time, the RPO is the **maximum amount of data loss that is acceptable**. Depending on the nature of the role, staff members may be able to recreate or re-enter data. RPO provides guidance on how to back up data, recovery policies, and whether loss prevention or correction is a better option.
  - **Work recovery time** (WRT)

Business Impact Analysis (BIA)

MTD, RTO, RPO and WRT

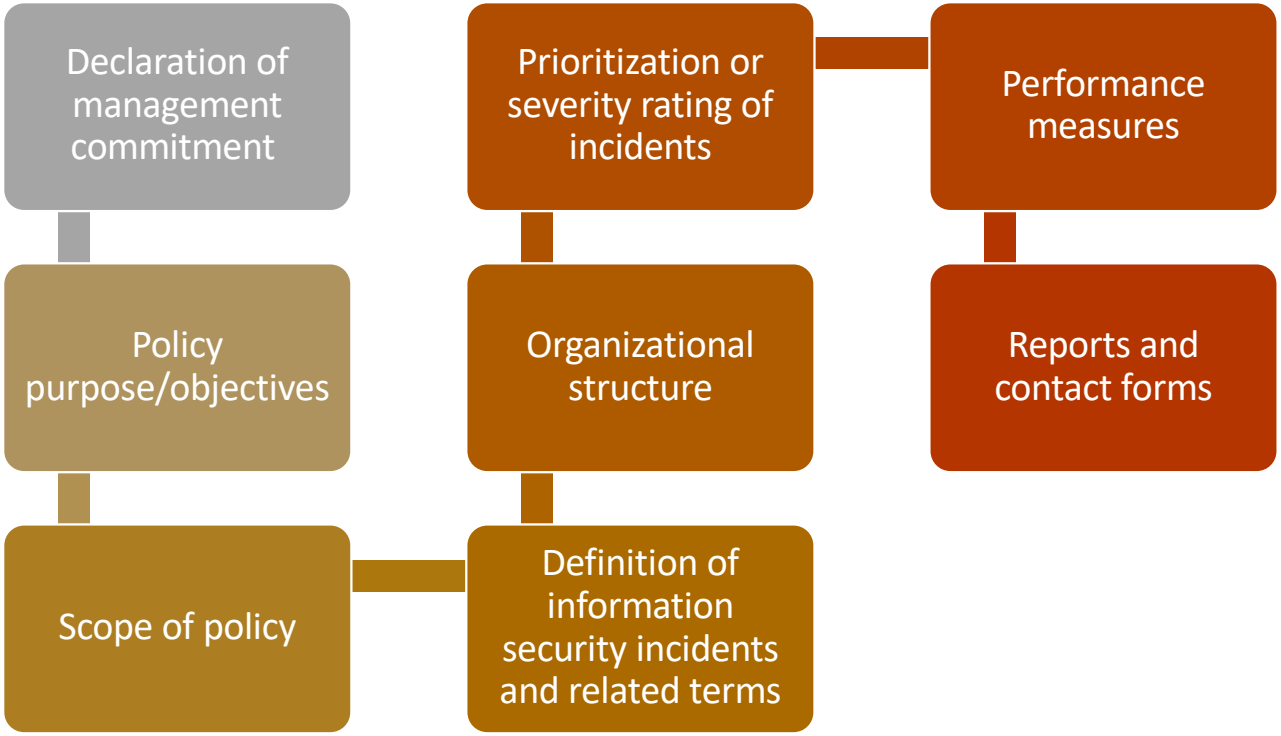


Incident Response Planning

- Planning the response to an incident **includes identifying, classifying, and responding to an incident**.
- **Attacks are classified** as **incidents** if they:
  - They are **directed against information** assets
  - Have a **realistic chance of success**
  - May **threaten** the **confidentiality**, **integrity**, or **availability** of information resources
- **Response to the incident** is **more responsive than proactive**, with the exception of the planning that must occur to prepare RI teams to be ready to react to an incident.

Incident Response Planning

⇢**Incident response policy** identifies the following **key components**



Incident Response Planning

- The **predefined responses** allow the **organization** to **react quickly** and **effectively** to the **detected incident**, if:
  - The organization has an incident response team
  - The organization can detect the incident
- The IR team consists of individuals needed to handle systems as the incident occurs.

- CSIRT – Computer Security Incident Response Team
- SOC – Security Operations Center

Incident Response Planning

Incident detection

- The most **common occurrence** is the complaint about technological support, often delivered to the helpdesk.
- **Careful training** is required to **quickly identify and classify** an **incident**.
- Once the incident is **properly identified**, the organization **can respond**.
- Incident indicators vary.

Incident Response Planning

- **Reaction** to incidents
  - It consists of actions that guide the organization to stop the incident, mitigate its impact and provide information for recovery
  - Actions that should occur **quickly**:
    - Notification of key personnel
    - Incident documentation
- Incident **containment** strategies
  - Containment of the scope or impact of the incident as a first priority; should then determine which information systems are affected by the
  - The organization can stop the incident and try to regain control through a number of strategies.

Incident Response Planning

Incident Recovery

- Once the incident is **contained and control of the systems recovered**, the next phase is **recovery**.
- The first task is to identify the necessary human resources and launch them into action.
- The full extent of the damage should be assessed.
- The organization re-addresses vulnerabilities, addresses any deficiencies in safeguards, and restores data and services from systems.

Incident Response Planning

Damage assessment

- Various sources of damage information can be used, including system logs, intrusion detection logs, configuration logs and documents, incident response documentation, and detailed system evaluation and data storage results.
- Computerised evidence must be carefully collected, documented and maintained in order to be used in formal or formal procedures.
- Individuals who assess harm need special training.

Incident Response Planning

- Automated response
  - New systems can respond autonomously to the threat of incidents.
  - The drawbacks of existing automated response systems can offset the benefits of.
    - Legal responsibilities of a counterattack
    - Ethical issues

Disaster recovery planning

⇢Disaster recovery planning (DRP) is the preparation and recovery of a **disaster**.

⇢The contingency planning team must decide which actions constitute **disasters** and which are **incidents**.

⇢When situations are classified as disasters, plans change how to respond; take steps to secure the most valuable assets to preserve long-term value.

⇢The DRP strives to restore operations at the primary site.

Business Continuity Planning

- Prepares the **organization to re-establish or relocate critical business operations during a disaster affecting operations at the primary site**

- If the **disaster** has made the **current location unusable**, there must be a **plan** to allow the **business to continue to function**.

- **BCP development is something simpler than IRP or DRP**
  - It consists mainly of selecting a continuity strategy and integrating in this strategy data storage and recovery functions off-site

Business Continuity Planning

- **Continuity strategies**
  - There are a number of strategies for business continuity planning.
  - The determining factor in selecting between options is usually **cost**.
  - In general, there are **three unique options**: "hot sites", "warm sites" and "cold sites".
  - **Three shared functions**: "time-share", "service bureaus" and "mutual agreements"”

Business Continuity Planning

Continuity strategies

OPTION	DESCRIPTION	COMMENTS
Hot site	Facility with environmental utilities, hardware, software, and data that closely mirrors the original data center	Most expensive option, least switchover time
Warm site	Facility with environmental utilities and basic computer hardware	Less expensive than a hot site but requires more time to load operating systems, software, data, and configurations
Cold site	Facility with basic environmental utilities but no infrastructure components	Least expensive option but at the cost of the longest switchover time, since all hardware, software, and data must be loaded at the new site
Mobile site	Trailer with necessary environmental utilities that can operate as a warm site or cold site	Very flexible, fairly short switchover time and widely varying costs based on size and capacity

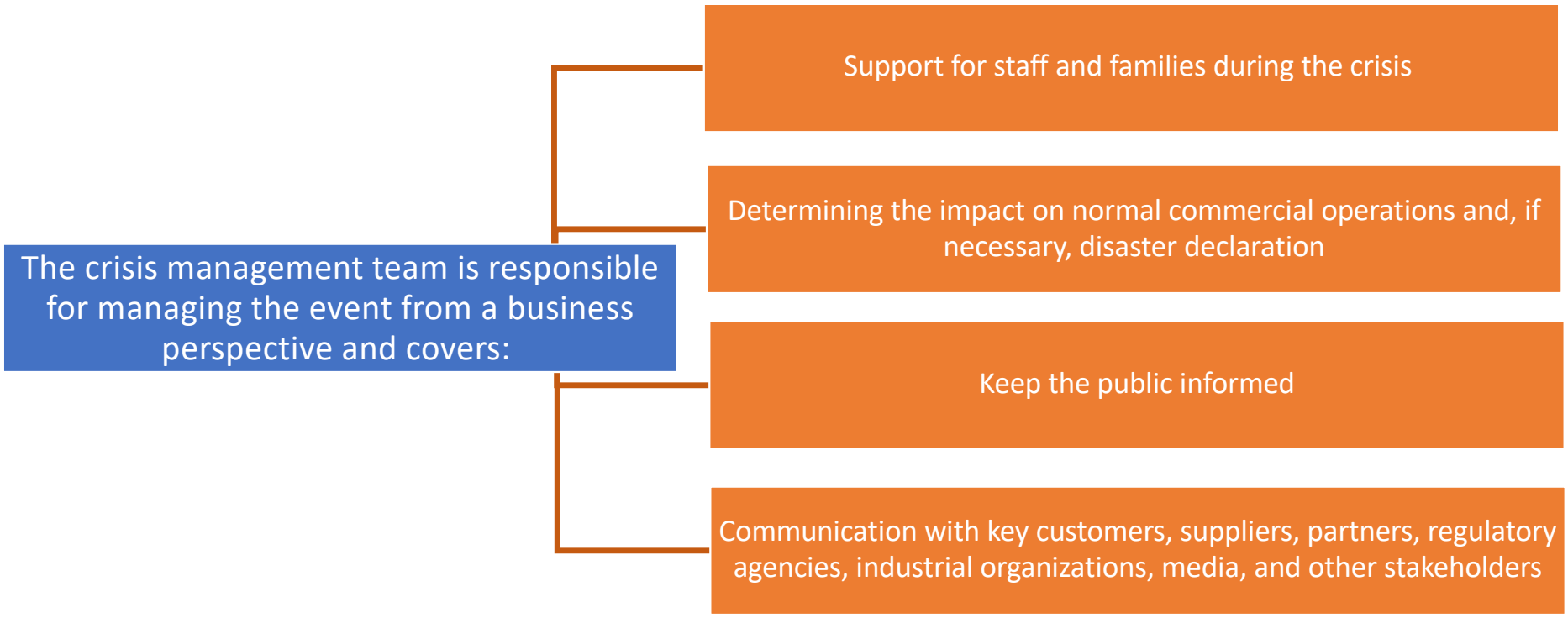
Business Continuity Planning

- Off-site disaster data storage
  - To get sites up and running quickly, an organization must have the ability to move data to new site systems.
  - Options for operating operations include:
    - Electronic vaults
    - "*Remote journaling*"
    - "Shadowing" of databases

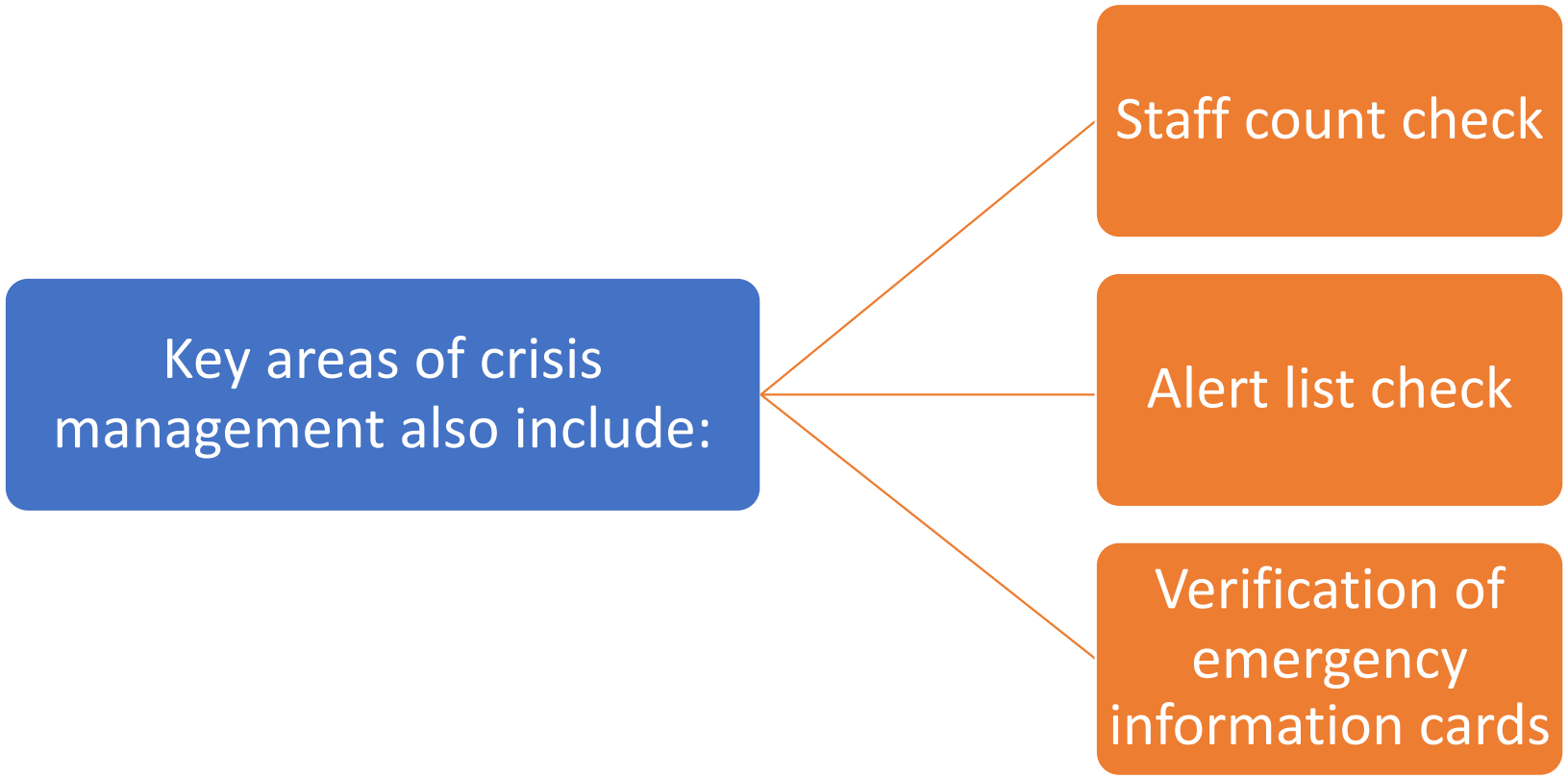
Crisis management

- **Actions** taken in **response to an emergency to minimize injury/loss of life**, **preserve the organization's image/market share**, and **complement disaster recovery/business continuity processes**
- What can really distinguish an incident from a disaster are the actions of response teams.
- Disaster recovery personnel should know their duties without any supporting documentation.
  - Preparation
  - Training
  - Rehearsal

Crisis management



Crisis management



The Consolidated Contingency Plan

- The single-set document approach combines all aspects of the policy and contingency plan, incorporating IR, DR, and BC plans.
- Often created and stored electronically, it should be easily accessible by employees in time of need.

Involvement of law enforcement services

- Where the **incident in question constitutes a violation of the law**, the organization may **determine that it is necessary to involve law enforcement**.
- Questions:
  - When should law enforcement get involved?
  - What level of law enforcement agency should be involved (local, state, federal)?
  - What happens when the law enforcement agency is involved?
- Some questions are best answered by the legal department.

Benefits and disadvantages of the involvement of law enforcement services

Advantages	Disadvantages
Agencies can be better equipped for proof processing	Once a law enforcement agency takes over the case, the organization cannot control the chain of events
The organization may be less effective in extracting the information needed to legally convict suspected criminals	The organization may not hear about the case for weeks or months
Law enforcement agencies are prepared to handle any necessary warrants and subpoenas	Vital equipment for the organization's business can be labelled as proof
Law enforcement is competent to obtain witness statements and to collect other information from	If the organization detects a criminal act, it is legally obliged to involve law enforcement officials

2022 | 2023

Network and Information Systems Security

Information Security Planning

Carlos Serrão
carlos.serrao@iscte-iul.pt

INSTITUTO UNIVERSITÁRIO DE LISBOA