



DAY 1

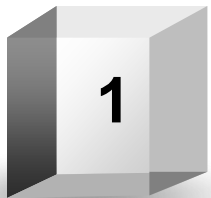
Certified ISO 27001  

---

Lead Implementer

# Training Objectives

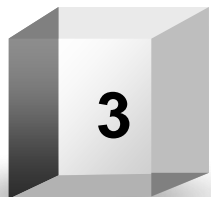
## Acquiring Knowledge



Understand the components and the operation of an Information Security Management System based on ISO 27001 and its principal processes



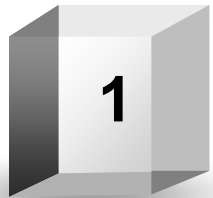
Understand the goal, content and correlation between ISO 27001 and ISO 27002 as well as with other standards and regulatory frameworks



Master the concepts, approaches, standards, methods and techniques for the implementation and effective management of an ISMS

# Training Objectives

## Development of Competencies



Interpret the ISO 27001 requirements in the specific context of an organization



Develop the expertise to support an organization to plan, implement, manage, monitor and maintain an ISMS as specified in ISO 27001

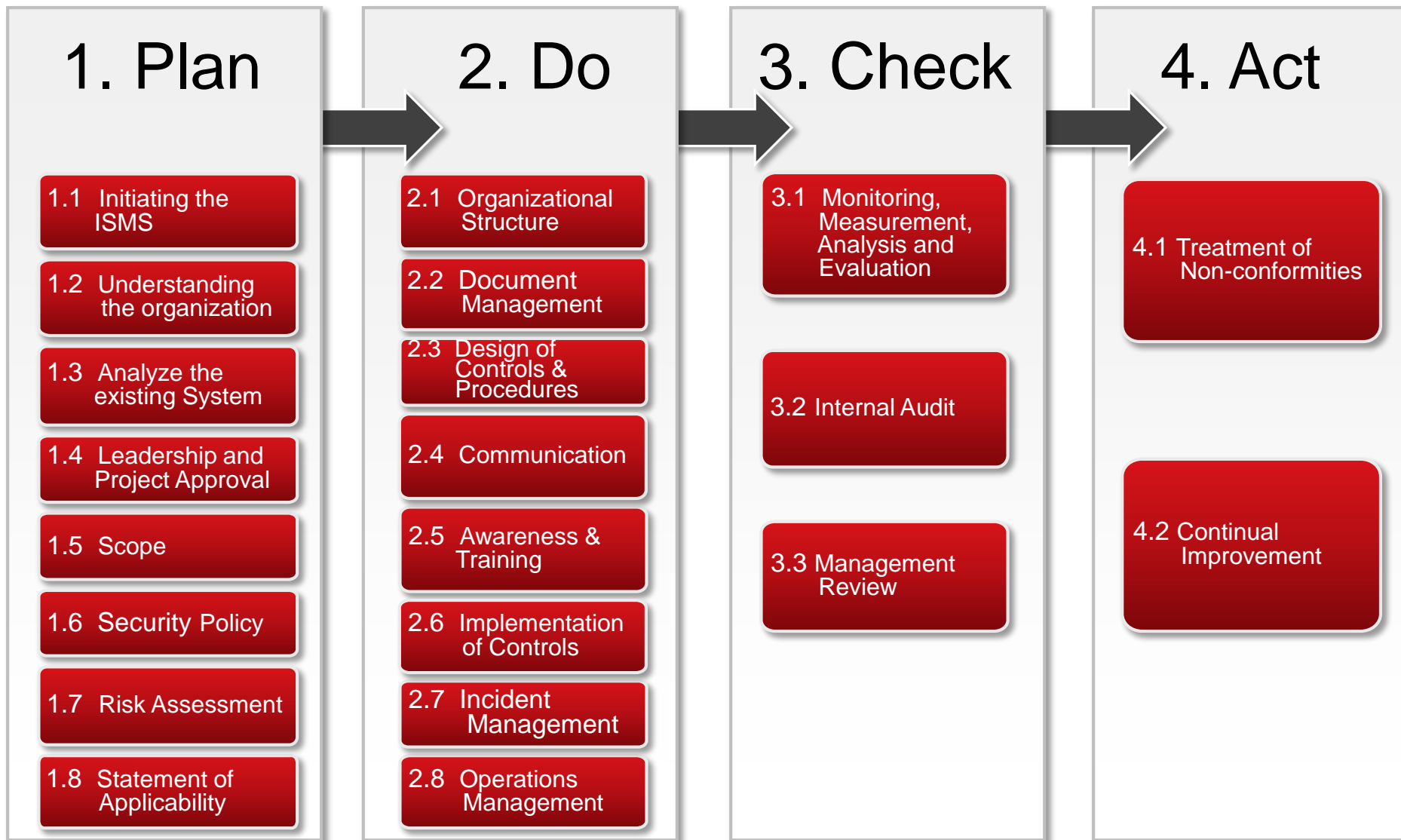


Acquire the expertise to advise an organization on information security management best practices



Strengthen the personal qualities necessary to act with due professional care when conducting a compliance project

# Choose a Methodological Framework to Manage the ISMS Implementation Project



# 1.1. Initiating the ISMS Implementation

## Proposed approach

### 1. Business Approach

Integrates into the context of commercial activities across the organization

### 2. Systems Approach

Overall implementation of the ISMS process, not by isolating processes

**Guidelines**



### 3. Systematic Approach

Apply best practices in project management

### 4. Integrated Approach

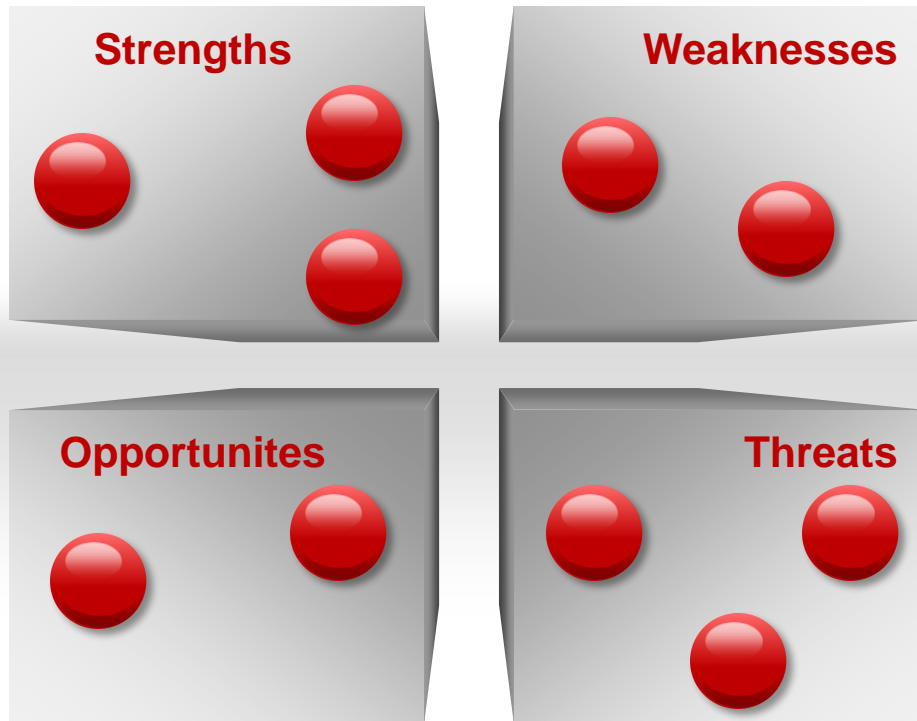
Integrating the ISMS or harmonize it with other requirements of the organization

### 5. Iterative Approach

Rapid implementation of the ISMS respecting the minimum requirements and switch to continuous improvement thereafter

# 1.2. Understanding the Organization and its Context

## Analyzing the External Environment



### Practical Advice

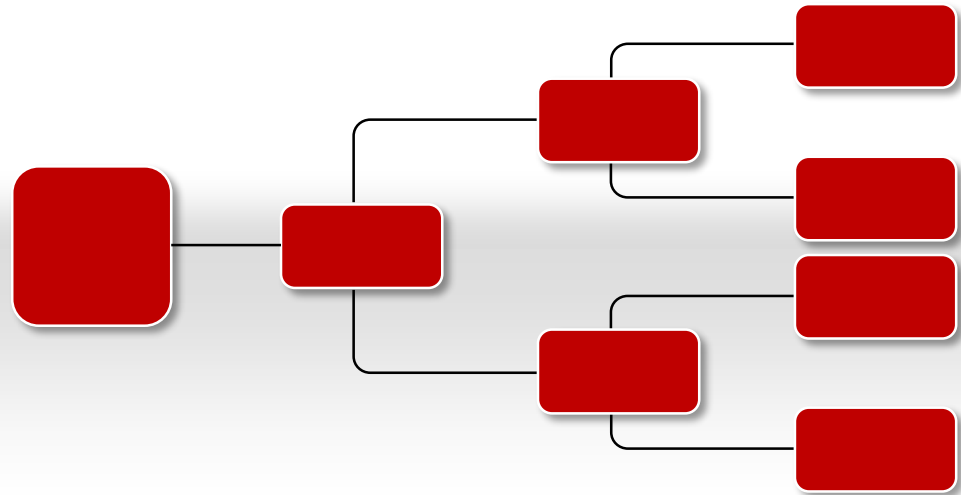
- ISO 27005 offers no practical approach to analyze the context of an organization
- Several methodologies exist to understand how an organization functions
- The important thing is to identify the characteristics of internal and external environmental factors that will influence risk management: mission, main activities, internal organization, stakeholders, etc..

# 1.2. Understanding the Organization and its Context

## Analyzing the Internal Environment

Understanding the structure and main actors of the organization related to the scope at the levels:

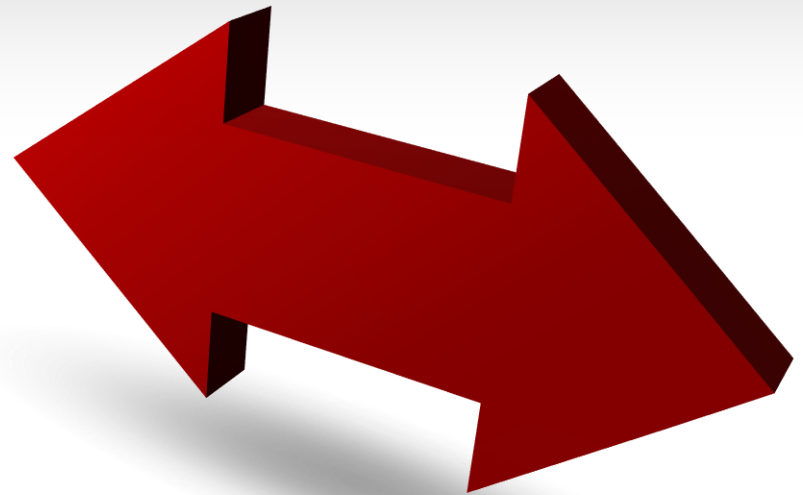
- Strategy (who sets the strategic directions?)
- Steering (who coordinates and manages the operations?)
- Operational (Who is involved in production and support activities?)



# 1.3. Analysis of the Existing Management System

## Gap Analysis

- Technique to determine the steps to move from current state to a desired future state
- 1. Comparison of the current performance of the security management system with the ISO 27001 requirements
- 2. Identifying the improvement needs
- 3. Basis for drafting the ISMS project plan

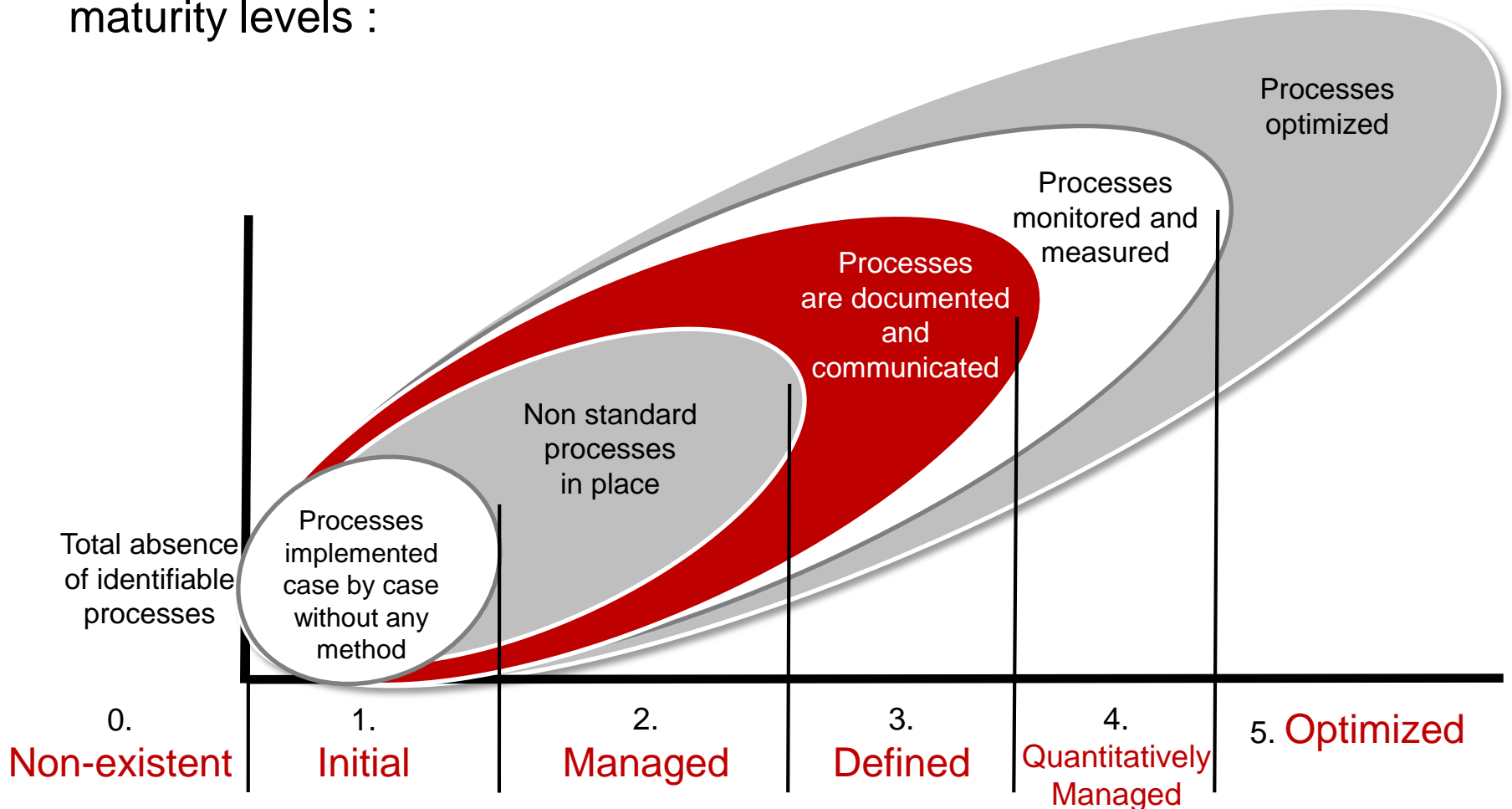




# 1.3. Analysis of the Existing Management System

## Gap Analysis and the Level of Maturity

You can set targets for processes and security controls based on target maturity levels :





DAY 2

Certified ISO 27001  

---

Lead Implementer

# 1.4. Leadership and ISMS Project Approval

ISO 27003, clause 5.4

## Key Benefits of Management Commitment

- Increased knowledge of laws
- Optimal allocation of resources
- Identification of critical assets
- Security process checked and measured



# 1.5. ISMS Scope

## Importance

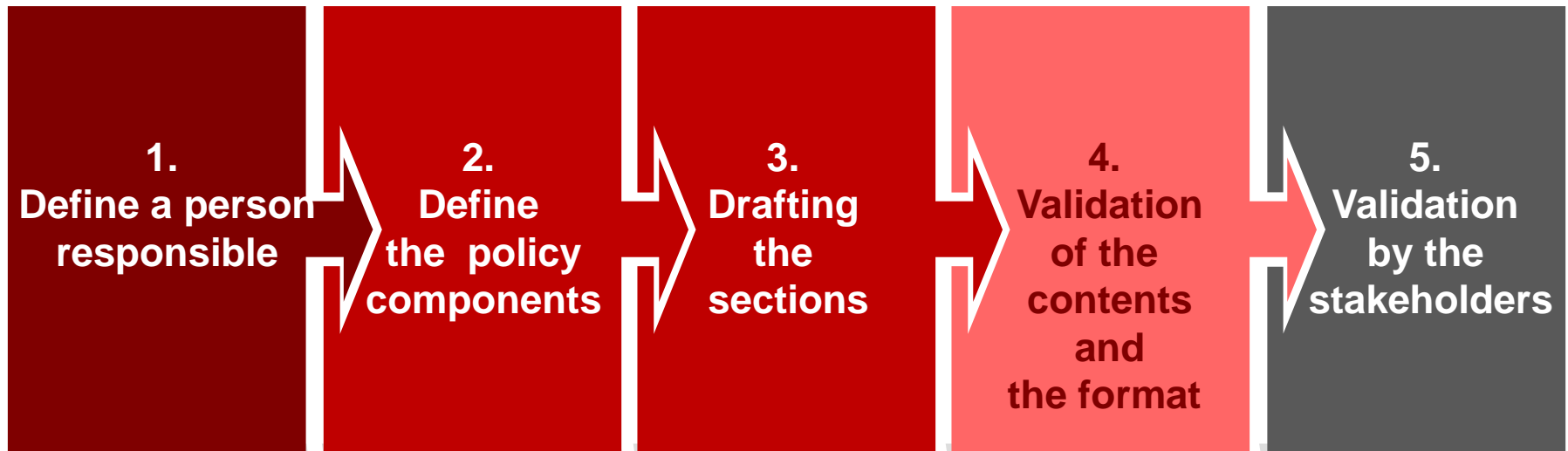
A clear definition of scope, focusing on key activities of the organization, is an important success factor for the ISMS implementation. This will make it easier to:

1. Get the support of the management
2. Mobilize stakeholders for the project
3. Justify added value to the interested parties

**Important note: the size of the scope is the first factor influencing the amount of effort required for the project**

# 1.6. ISMS Policy

## Process of Drafting a Policy



- it is important to ensure the support and understanding of a policy before its publication

# 1.6. ISMS Policy

## Types of Policies

### High level General Policies

- General guidelines for the management of a sector of activities: procurement & supply, human resources, sales, marketing, etc.

Security Policy

### High Level Topic-specific Policies

- Specific guidance on a topic

Information Security Policy

ISMS Policy

### Detailed Policies

- Specifies the internal requirements of another policy
- Usually covers a very specific and / or target audience

Policy on access control

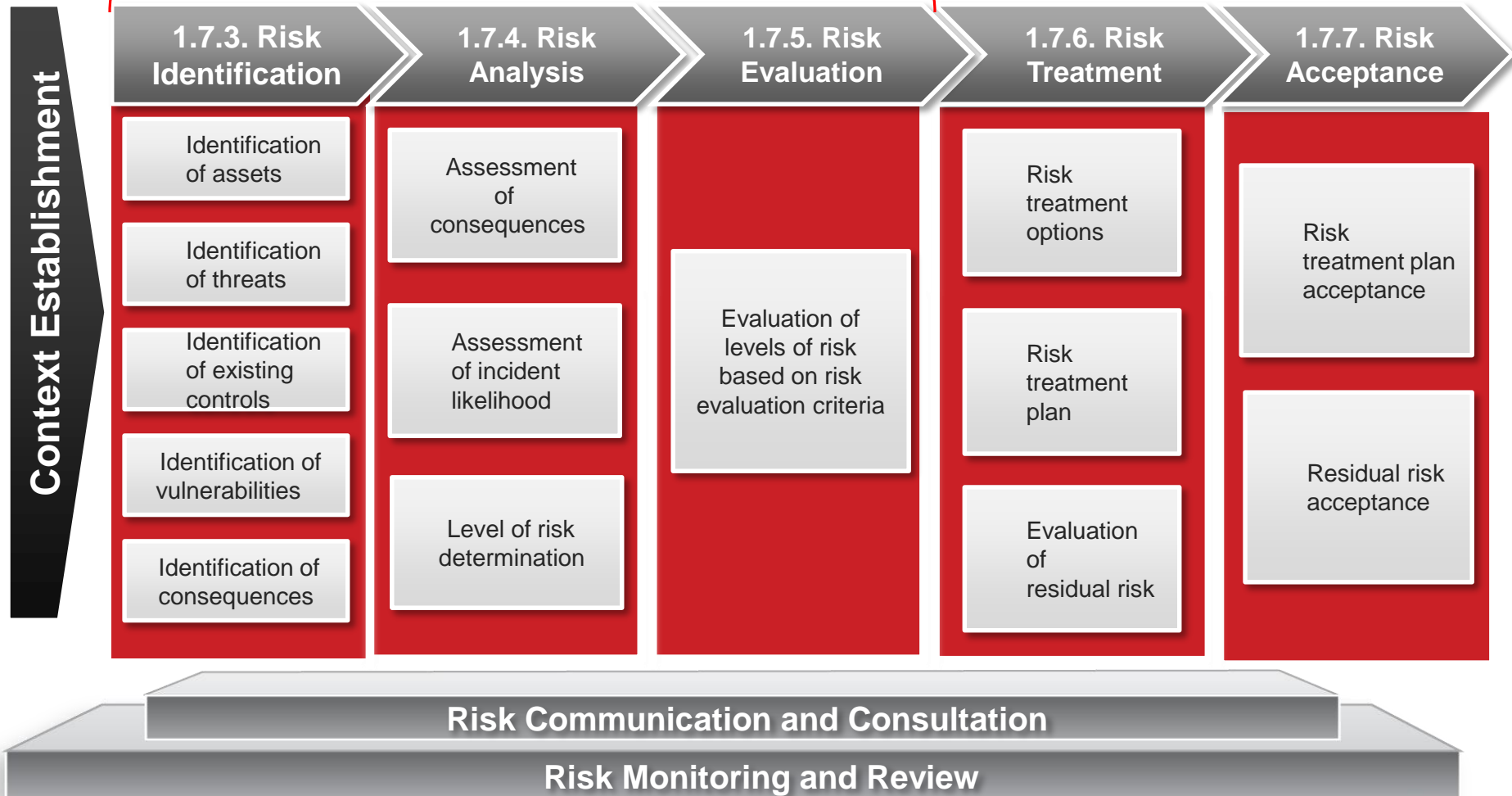
Policy on cryptography

Incident Management Policy

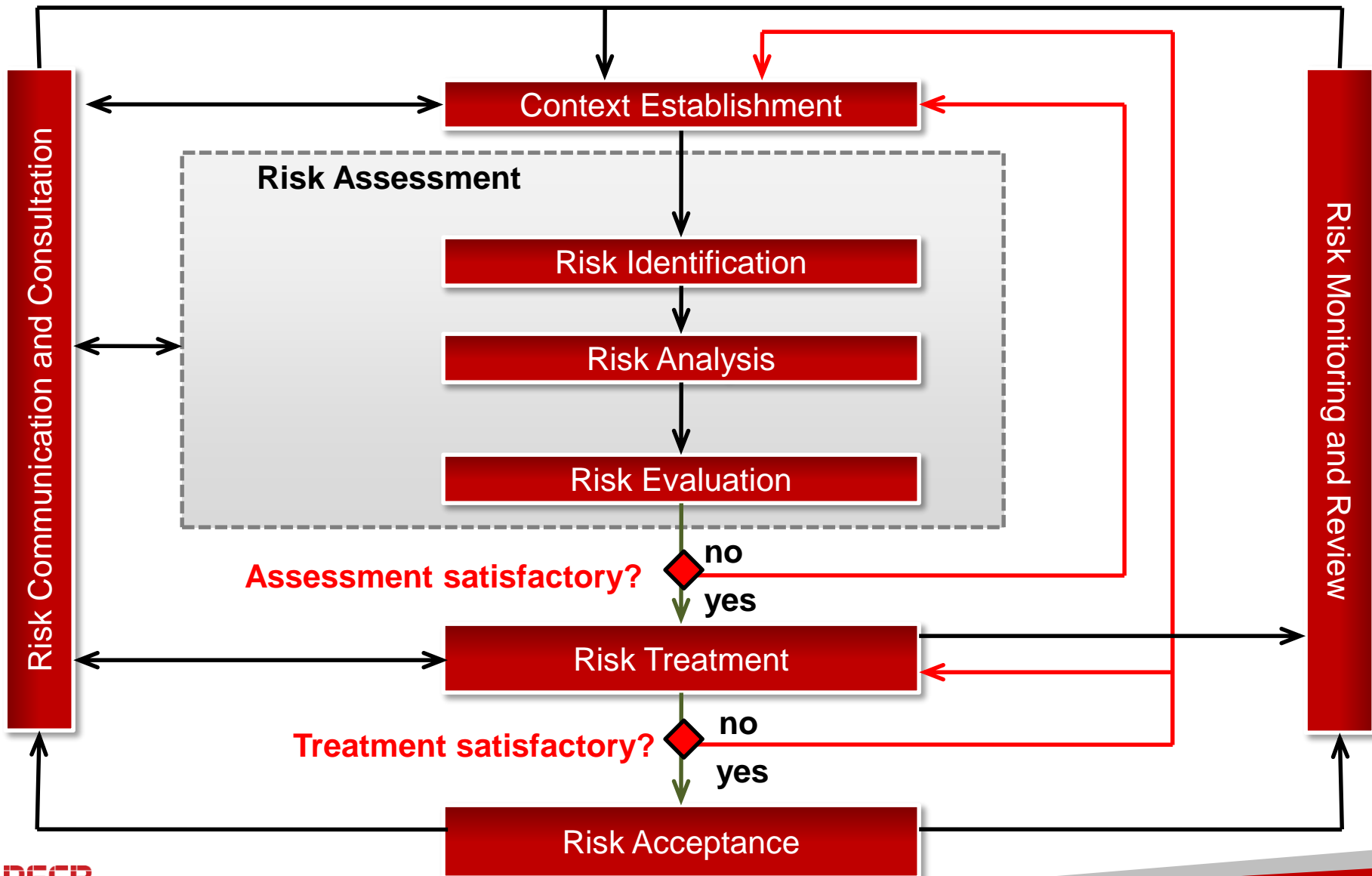
Policy on Continuity of activities

# 1.7. Risk Assessment

## *Risk Assessment*



# 1.7. Information Security Risk Management Process according to ISO 27005





# 1.8. Statement of Applicability

## Example

Control	Applicable	Description	Justification	Documentation	Responsible
A.5.1.1. Information security policy document	yes	The Information Security policy, approved by management, in effect since December 21, 2008. A copy was sent to all employees and stakeholders. The official version is available on the Intranet	To provide to the information security guidance and support from management, according to business requirements and laws and regulations	Security-policy-3213PO	Information Security manager
A.5.1.2. Review of the information security policy	yes	Security policy information is reviewed each year at the management review and the formal resolution extended for another year. In case of major changes, a review may take place during the year at the request of RSI or direction	Ensure that security policy is kept up to date and remains aligned with the objectives of the organization	1. Mnagement-review-procedure-312PR 2. Security-policy-3213PO, Clause 6.2 3. Management Review Proceedings 2009	Information Security manager
A.6.2.2 Teleworking	No	-----	Our organization has no activities related to teleworking.	No document	IT manager



DAY 3

Certified ISO 27001  

---

Lead Implementer

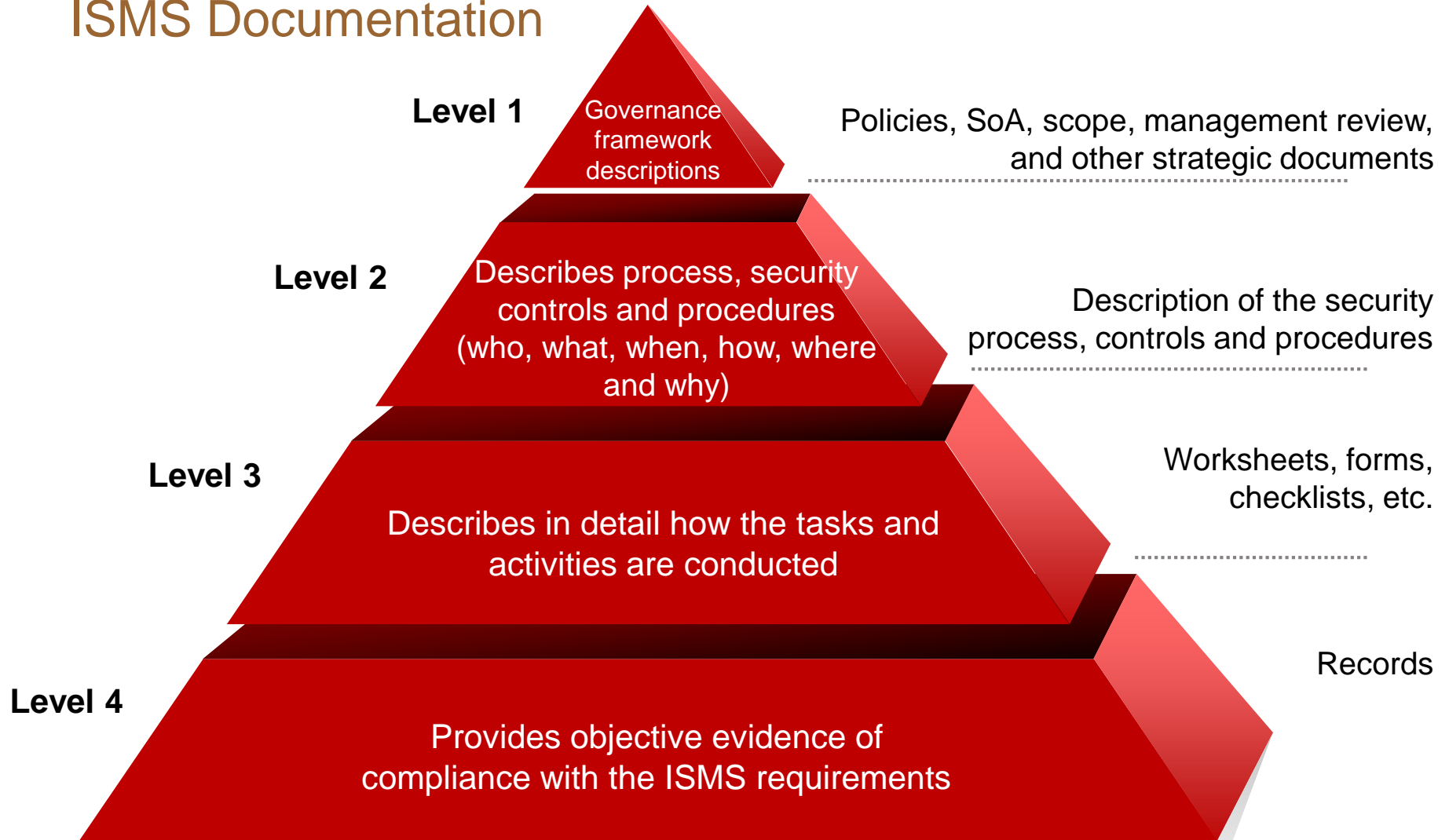
# 2.1. Organizational Structure

## Responsible for a Security Process or a Security Control

What are the missions?	How to implement?	When?
Determine the objectives for the process/control	Discuss with management, the head of information security and involved staff	Once a year
Being a "relay" between the information security responsible and all those involved in the process/controls operations	<ul style="list-style-type: none"> <li>- Communicate and educate on issues of the ISMS process</li> <li>- Encourage reporting of incidents, malfunctions, suggestions for improvement, etc</li> <li>- Communicate the decisions of the information security committees and the management reviews</li> </ul>	Ongoing
Ensure the proper functioning of the process/controls and availability of all related documentation	Verify that the processes and controls are applied every day	Ongoing
Ensure compliance of documentation with reality (file process, records, procedures and other related documents)	Taking into account the audits results, the reports of the information security committee and the feedback from stakeholders	Ongoing
Ensure the availability of information to monitor and measure the process	Check that the elements defined in the monitoring table of objectives and monitoring are available	According to the periodicity of indicators
Follow the treatment of non-conformities, corrective and preventive actions on the process	Verify that the monitoring table notification forms are properly filled in	After each reporting

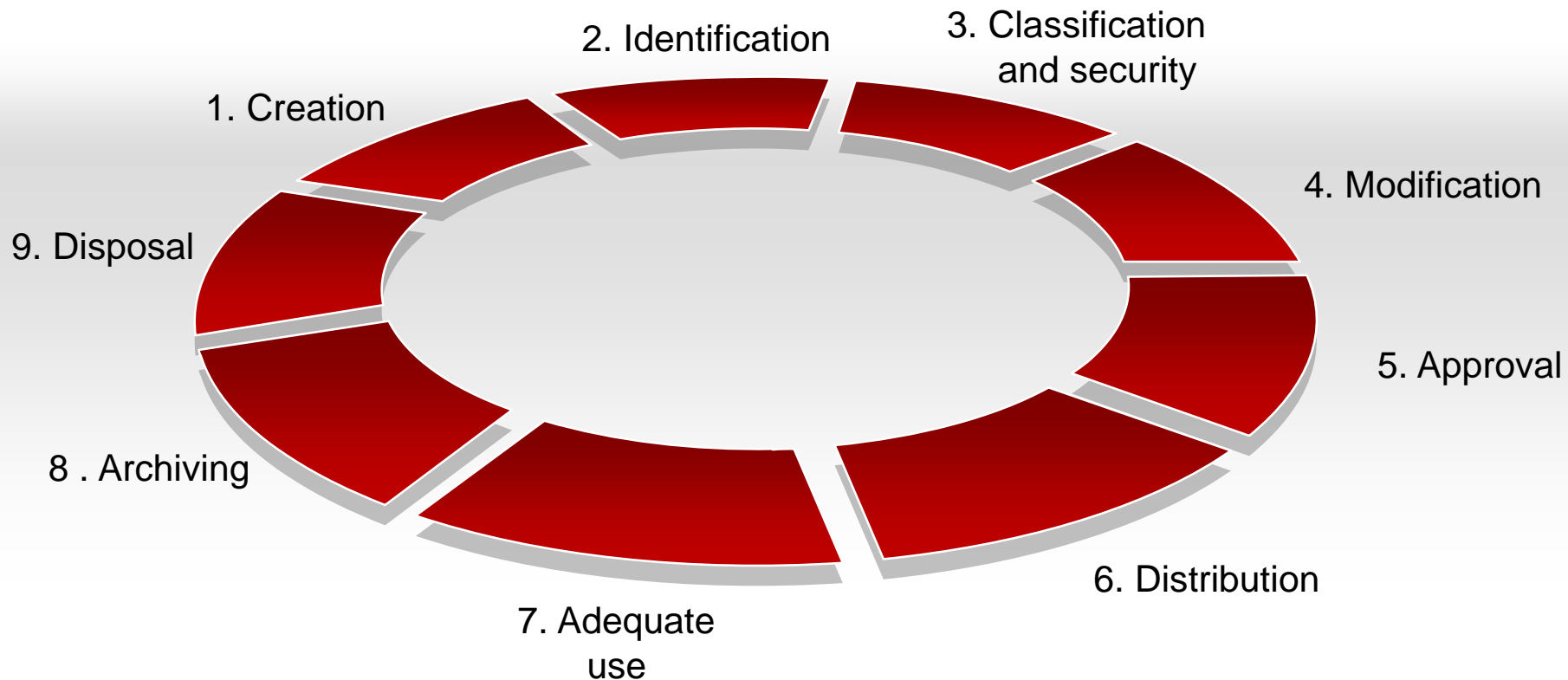
# 2.2. Documentation Management

## ISMS Documentation



## 2.2. Documentation Management

Developing a documentation management process and drafting of a procedure



A procedure must be established to manage the document life cycle

## 2.3. Design of Controls & Procedures

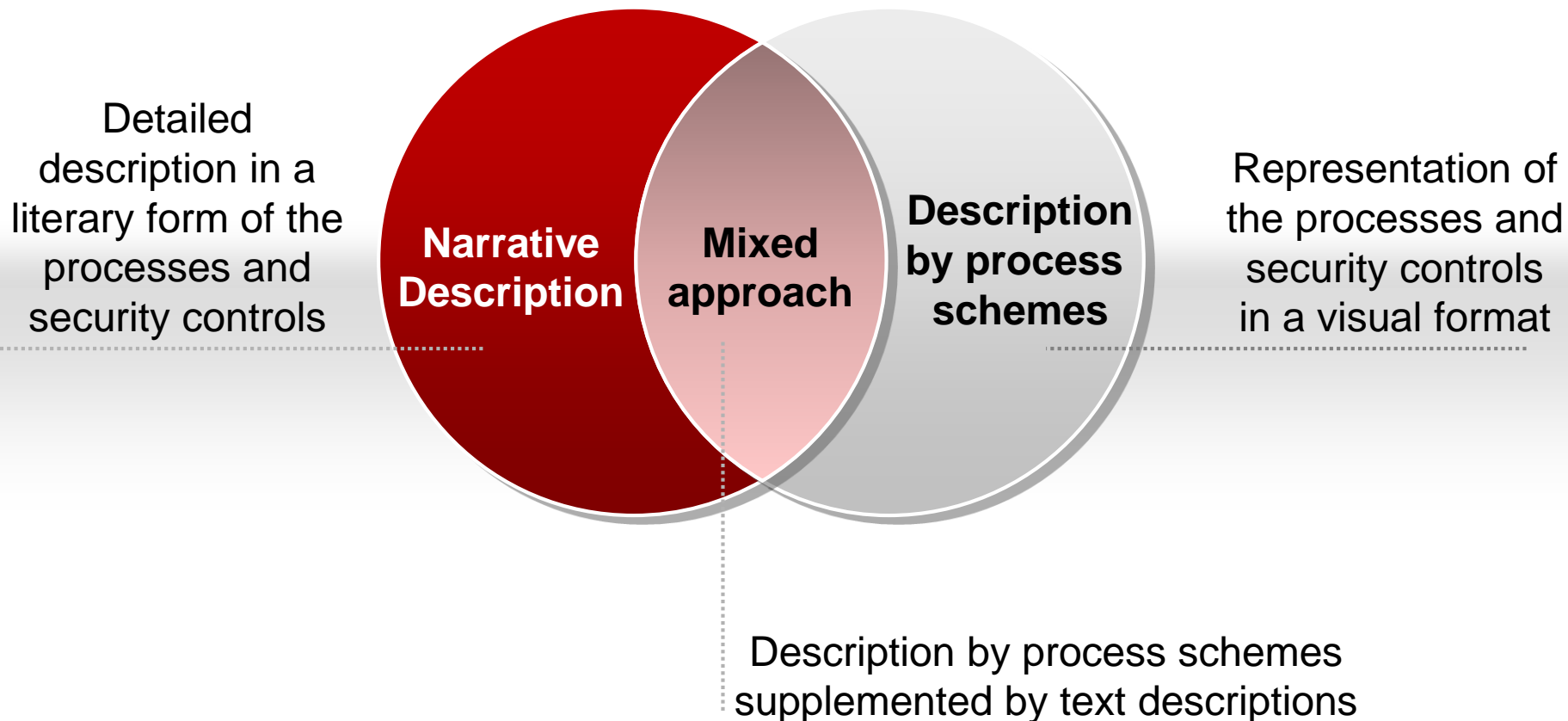
### Designing the Processes and Controls

Before describing the processes and controls they should be thought up and the design should be "carried out" by identifying:

1. Objectives
2. The elements entered
3. The roles and responsibilities of key stakeholders
4. Interfaces with other processes
5. The resources needed for operations
6. Lists of activities and tasks to perform in operations
7. List of records
8. Key indicators of efficiency measures
9. Output elements

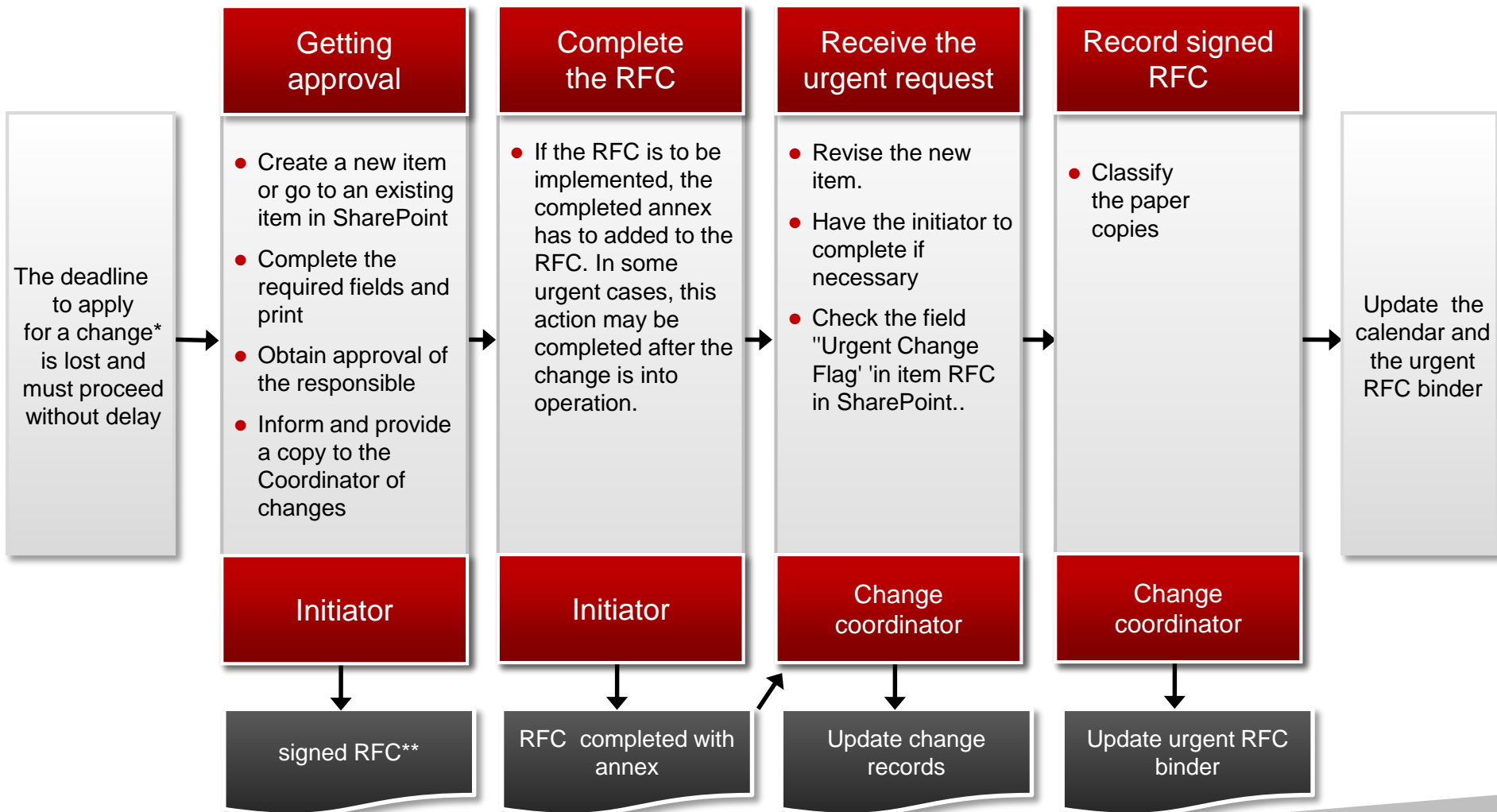
## 2.3. Design of Controls & Procedures

### Description of the Processes and Controls



# 2.3. Design of Controls & Procedures

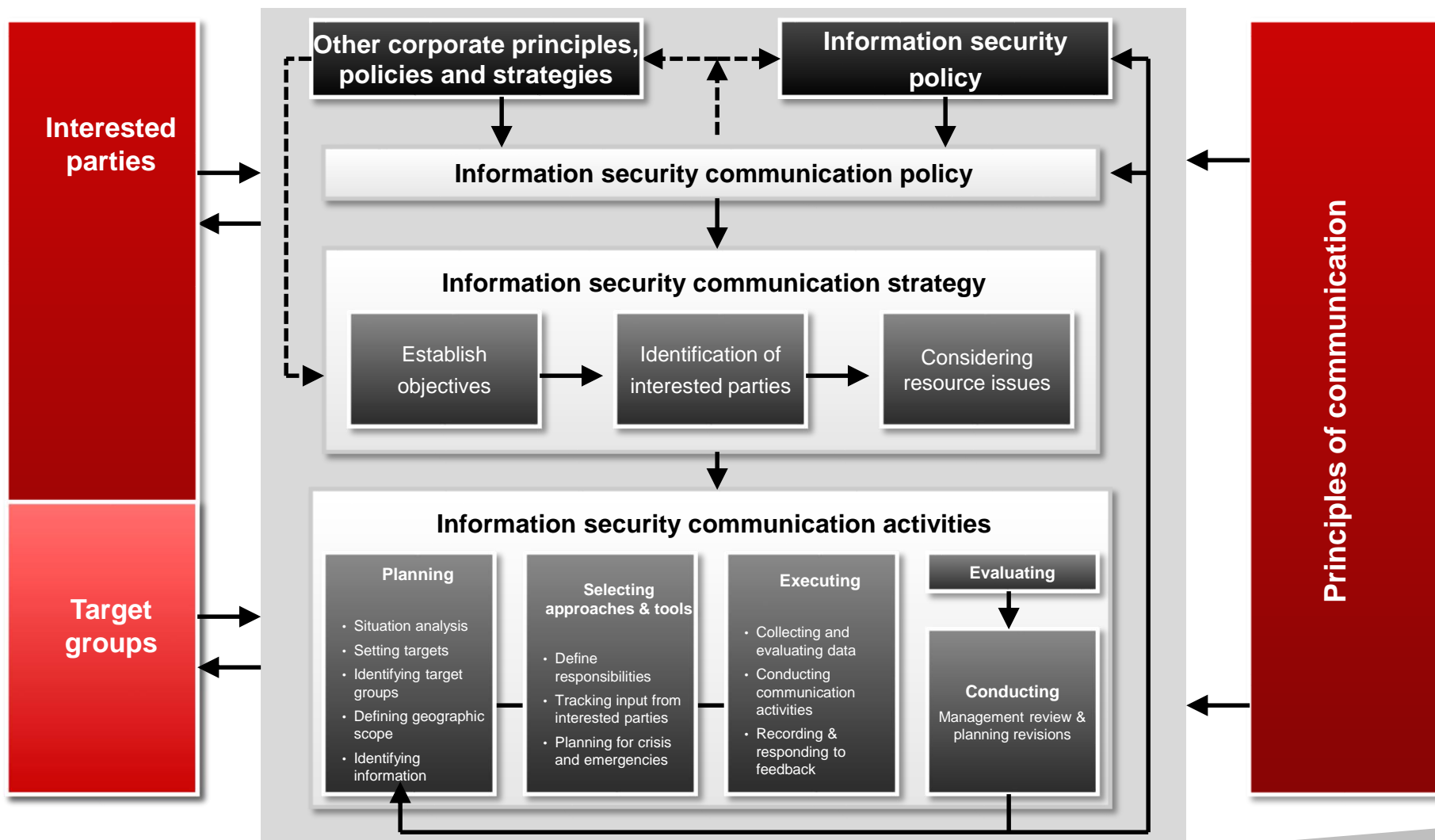
## Example of an application process for an urgent change





# 2.4. Communication

## ORGANIZATION



# 2.4. Communication

## Communication approaches and tools

Website

Newspaper articles

Surveys

Reports

Press releases

Guided tours  
of the organization

brochures &  
newsletters

Advertisement

Workshops  
and Conferences

Posters

Public meetings

Media interviews





Emails

Focus group

Presentation to groups

# 2.5. Awareness and Training

## Assessment of the required Skills

Functions	Policies	Incident	Risk	Audit	Legal
Function A					
Function B					
Function C					
Function D					
Function E					



Expertise



Knowledge



Awareness-Level

# 2.5. Awareness and Training

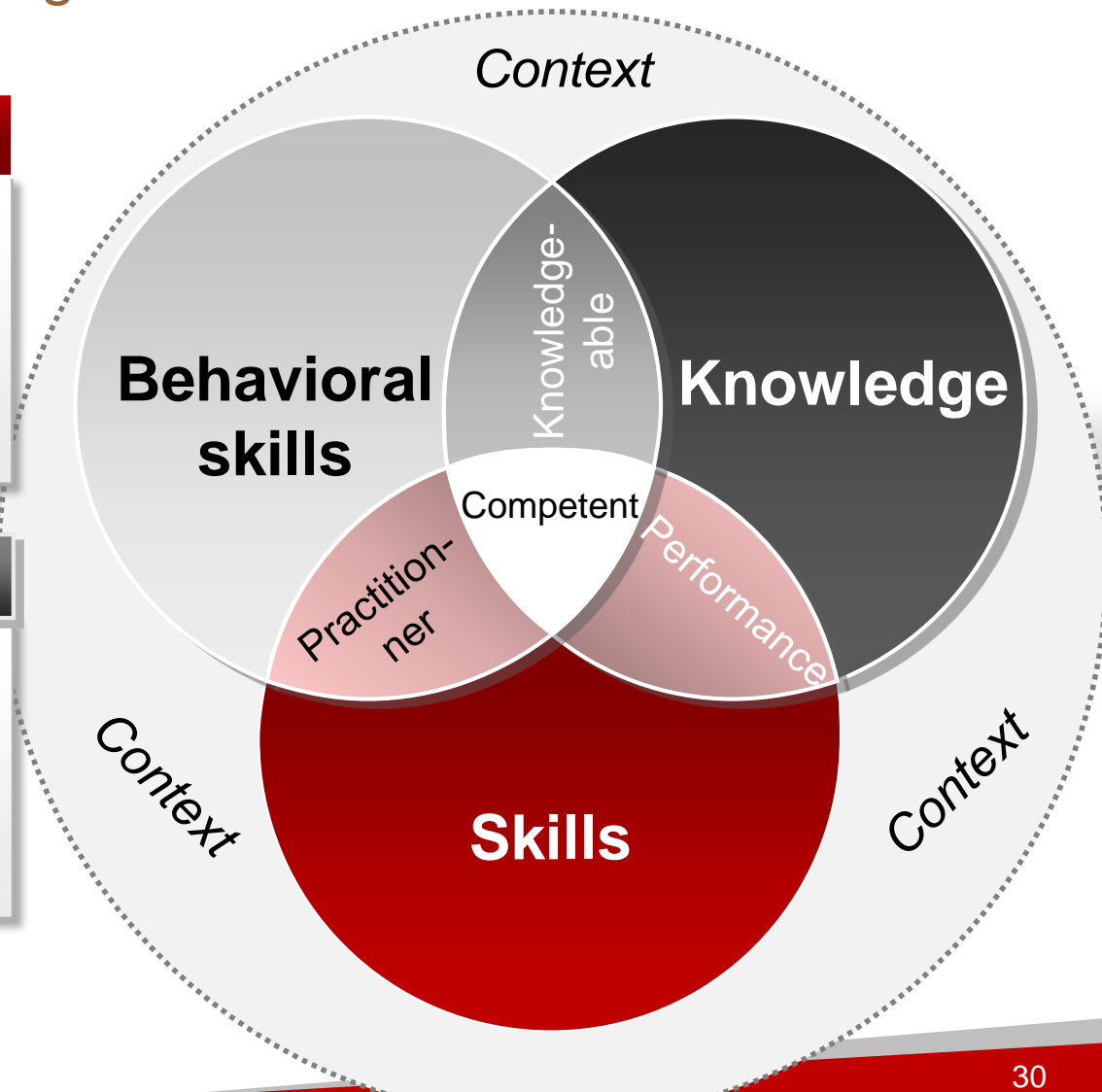
## Competence and Training

### Competence

- Demonstrated ability to implement knowledge and skills

### Training

- Process to provide and develop knowledge, skills and behavior to meet requirements



## 2.5. Awareness and Training

The awareness program allows:

1. To raise awareness
2. To ensure consistency in Information security practices
3. To contribute to the dissemination and implementation of policies, guidelines and procedures



**An employee who is not aware or untrained represents a potential risk**

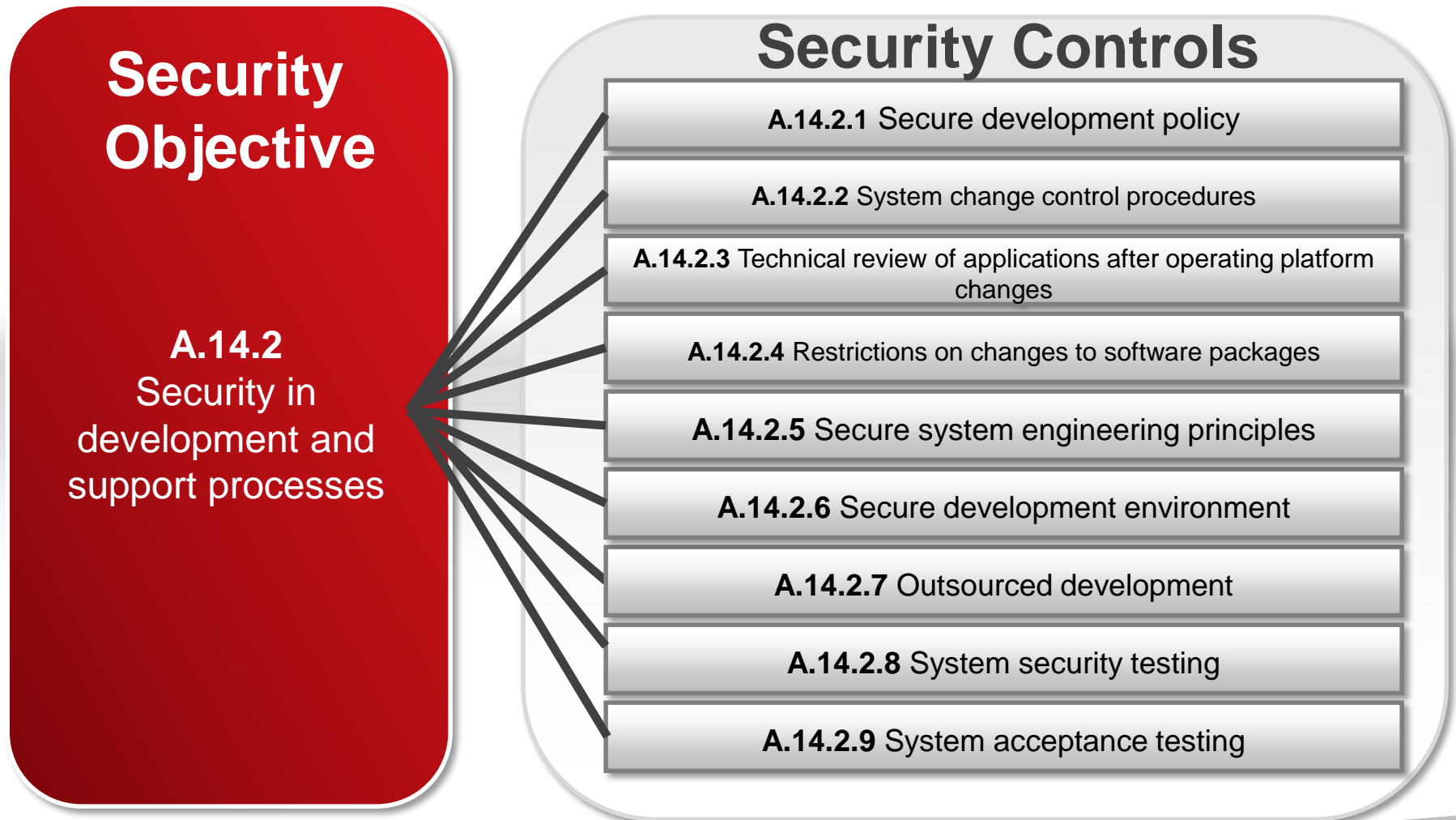
# 2.5. Awareness and Training

## Differences

<b>Training</b>	<b>Awareness</b>	<b>Communication</b>
Acquiring skills	Changing habits	Be informed
Addressed to the intellect	Intended primarily to emotions and behavior	Addressed to the intellect
What skills do they have to acquire?	What behavior do we want to strengthen or change?	What messages do we send?

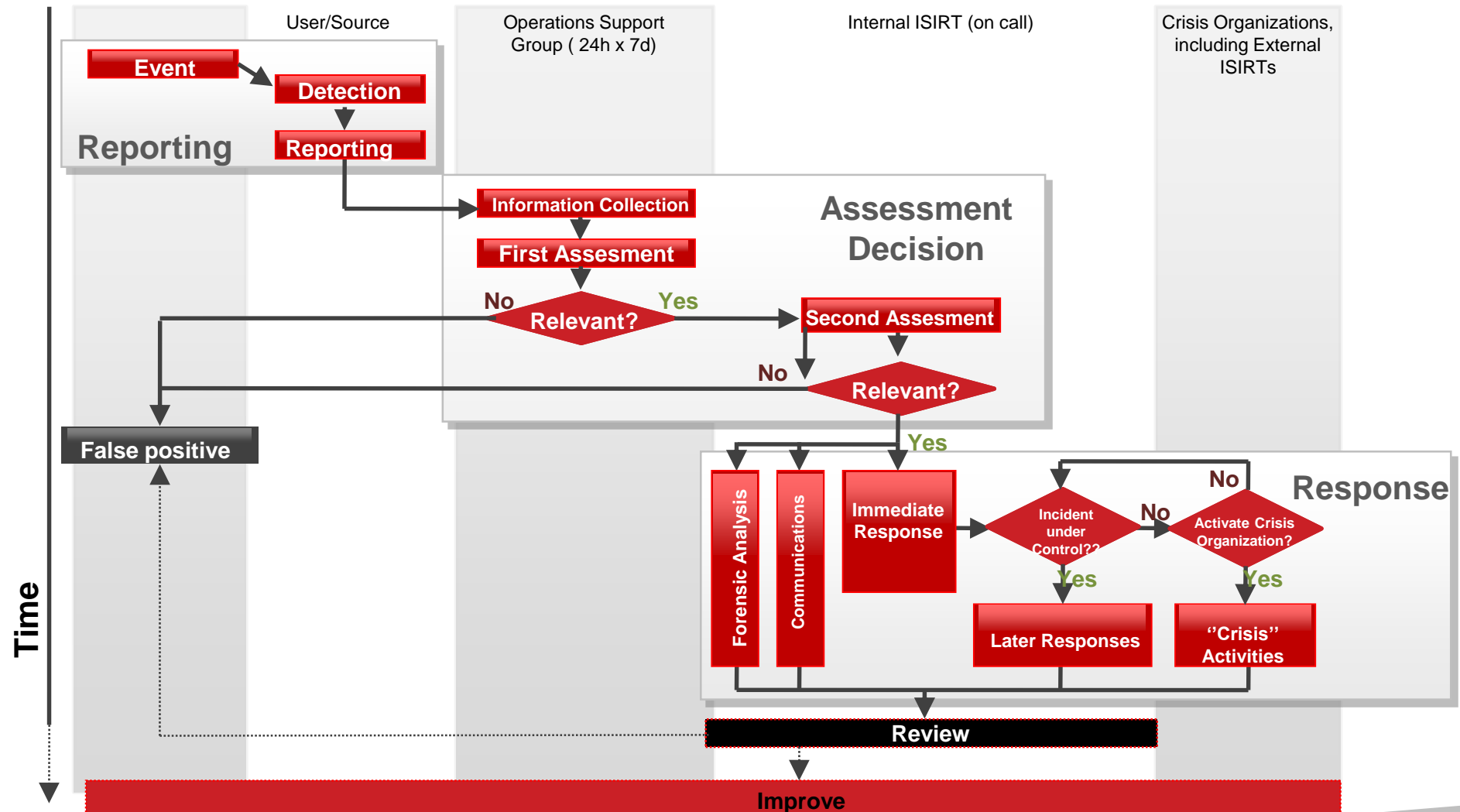
# 2.6. Implementation of Controls

ISO 27001, A.14.2



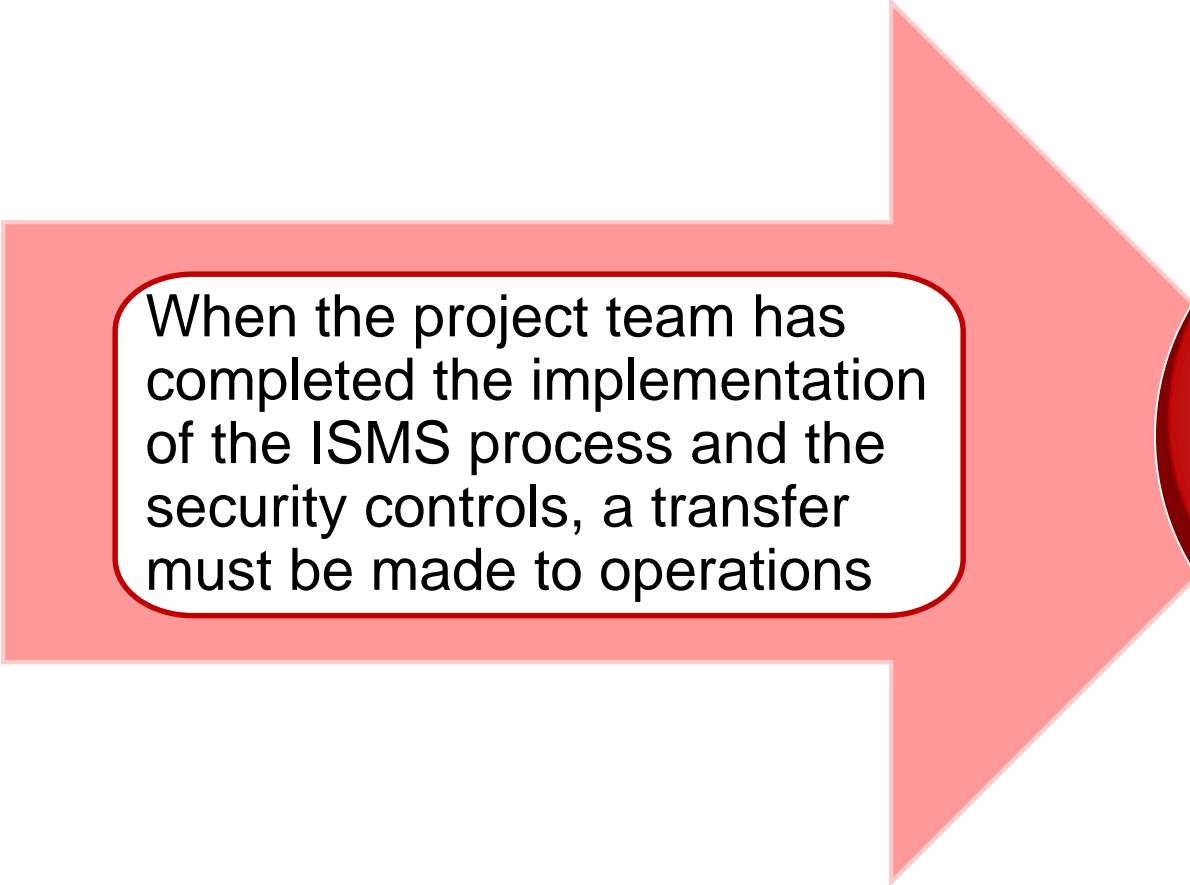
# 2.7. Incident Management

## Process and Procedure for Incident Management





## 2.8. Operations Management



When the project team has completed the implementation of the ISMS process and the security controls, a transfer must be made to operations



**Management  
of  
Operations**



# Day 4

Certified ISO 27001  
Lead Implementer

# 3.1. Monitoring, Measurement, Analysis and Evaluation

## Determination of measurement objectives

### Measurement Objectives

- The standard does not indicate what needs to be monitored or measured
- It is up to the organization to determine what it needs to be monitored and measured
- It is best practice to focus monitoring and measurement on the activities that are linked to the critical processes that enable the organization to achieve its information security objectives and targets
- Too many measures can distort an organization's focus and blur what is truly important



# 3.1. Monitoring, Measurement, Analysis and Evaluation

## What minimally needs to be monitored and measured?

1. The extent to which the organization's information security policy, objectives and targets are met

2. The processes, procedures and functions that protect its prioritized activities



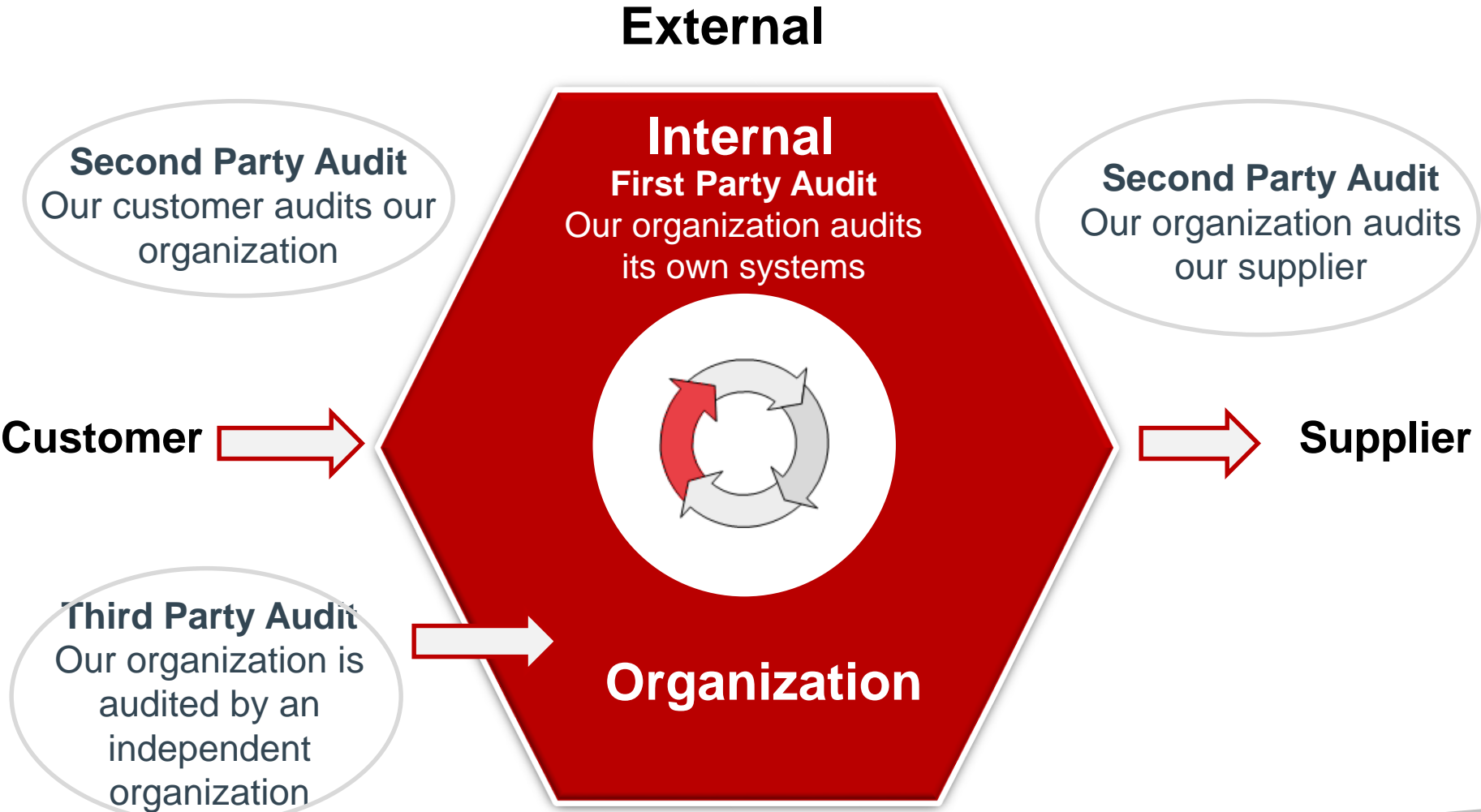
5. Data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventive action analysis

3. Historical evidence of deficient ISMS' performance, e.g. nonconformity, near misses, false alarms, failures, incidents

4. Compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own information security management policy and objectives

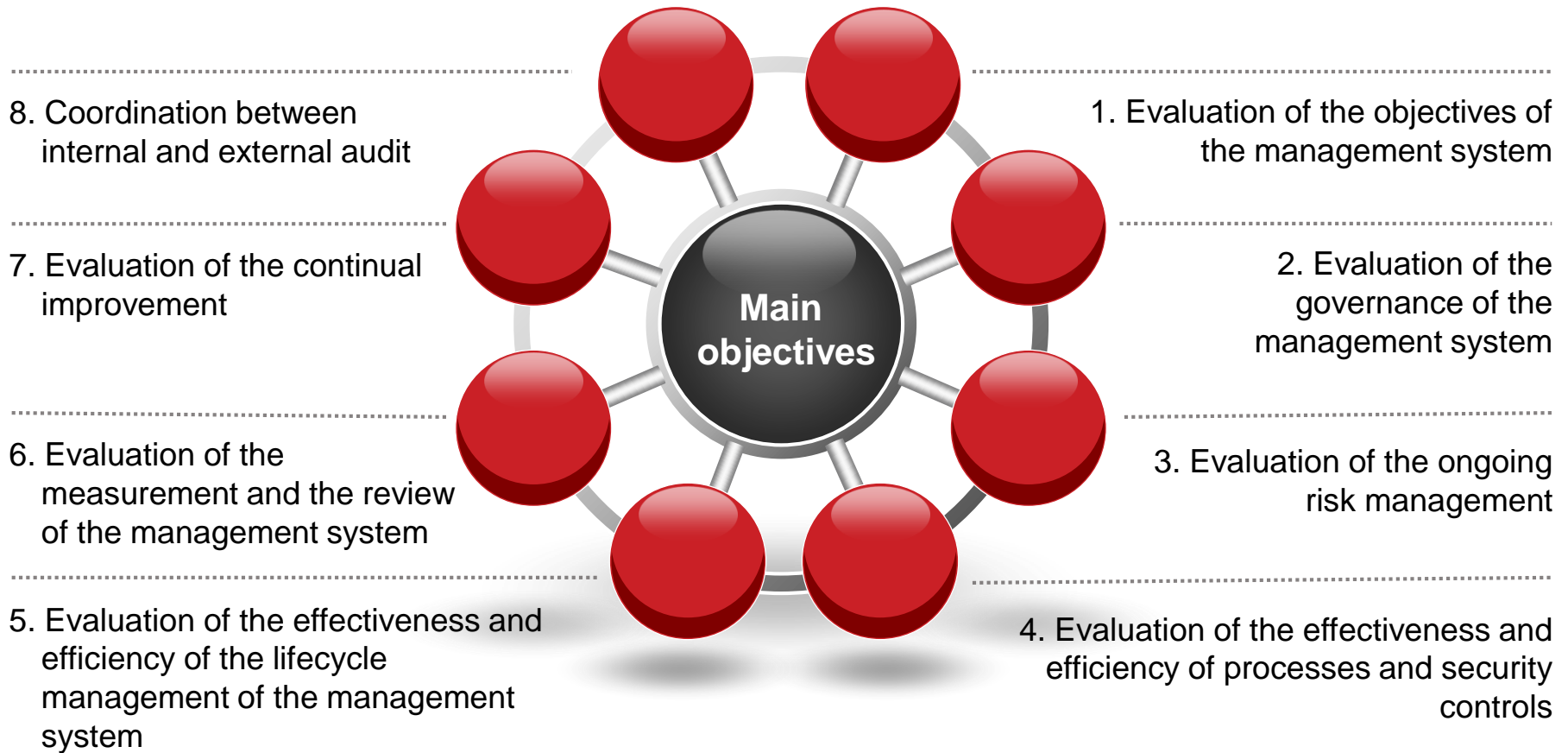
# 3.2. Internal Audit

## Types of Audits



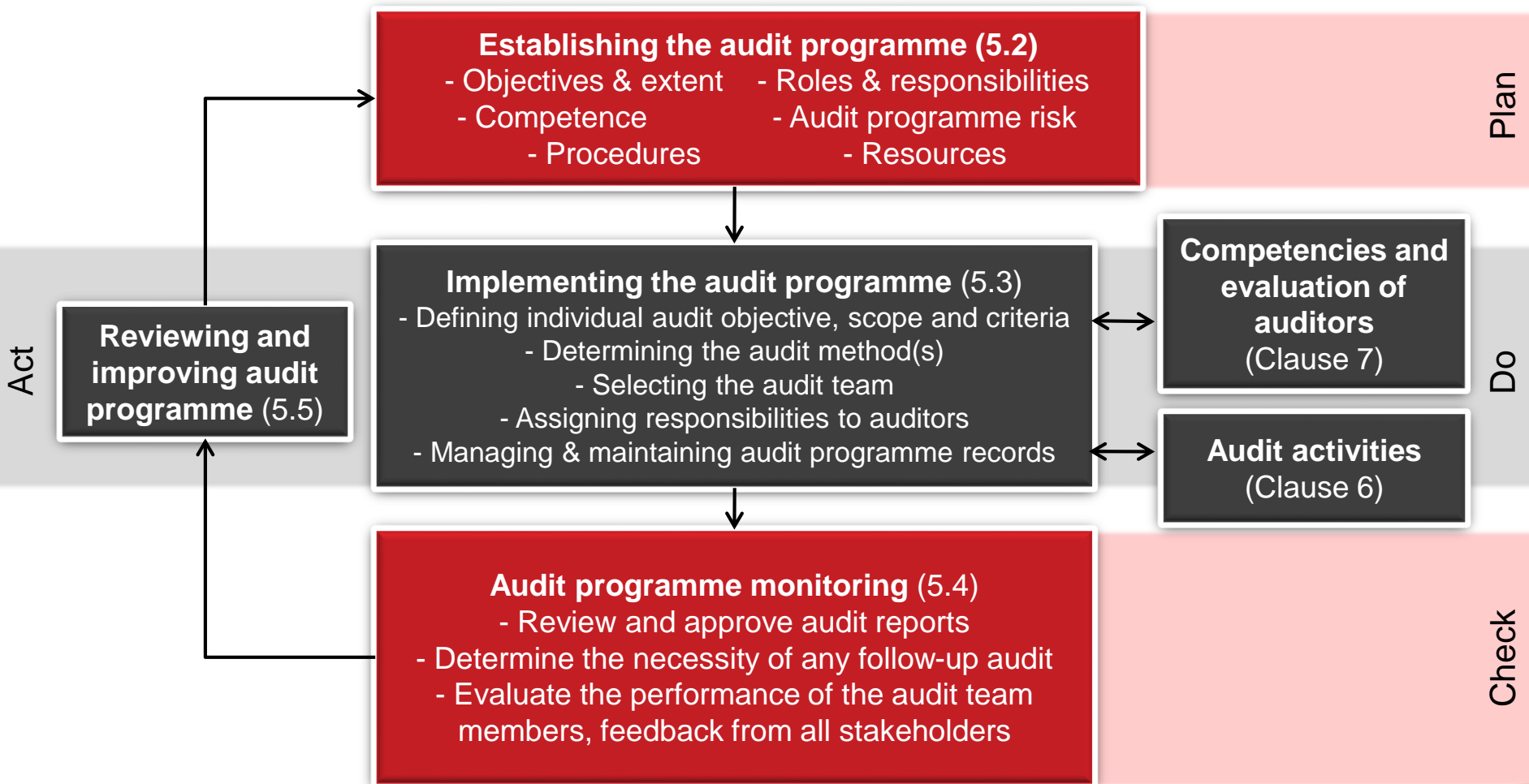
# 3.2. Internal Audit

## Main Services and Activities of the Internal Audit



# 3.2. Internal Audit

## Create the Internal Audit Programme



# 3.2. Internal Audit

## Create Audit Procedures

**Audit procedures should include information on how to:**

1. Plan and schedule audits considering audit risks

4. Select appropriate audit teams and assign their roles and responsibilities

7. Report the outcome of the audit programme to the audit client

2. Manage information security and confidentiality and manage the audit risks

5. Conduct audits, including the use of appropriate sampling methods

8. Maintain audit programme records

3. Assure the competence of auditors and audit team leaders

6. Conduct audit follow-up, if applicable

9. Monitor the operation, risks and effectiveness of the audit programme

**For small organizations, the above activities can be covered by a single procedure**



# 3.3. Management Review

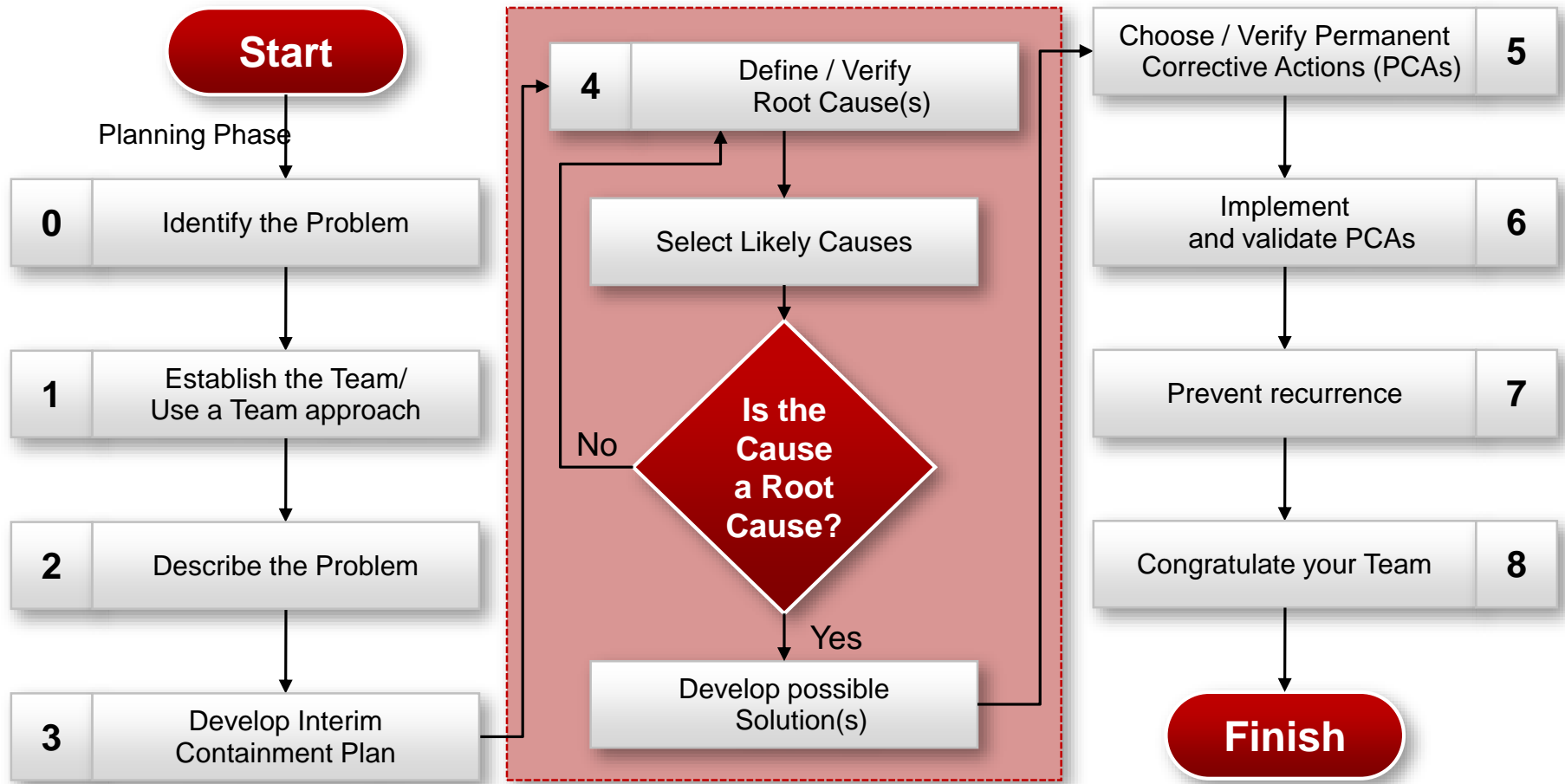
## Definition

A periodic review of the Management System performed by top management to analyze its continuing suitability, adequacy and effectiveness

Term	Concept
Suitability	Results are achieved in the best possible way
Adequacy	Outputs fulfill established criteria
Effectiveness	The system fulfills the organization's needs

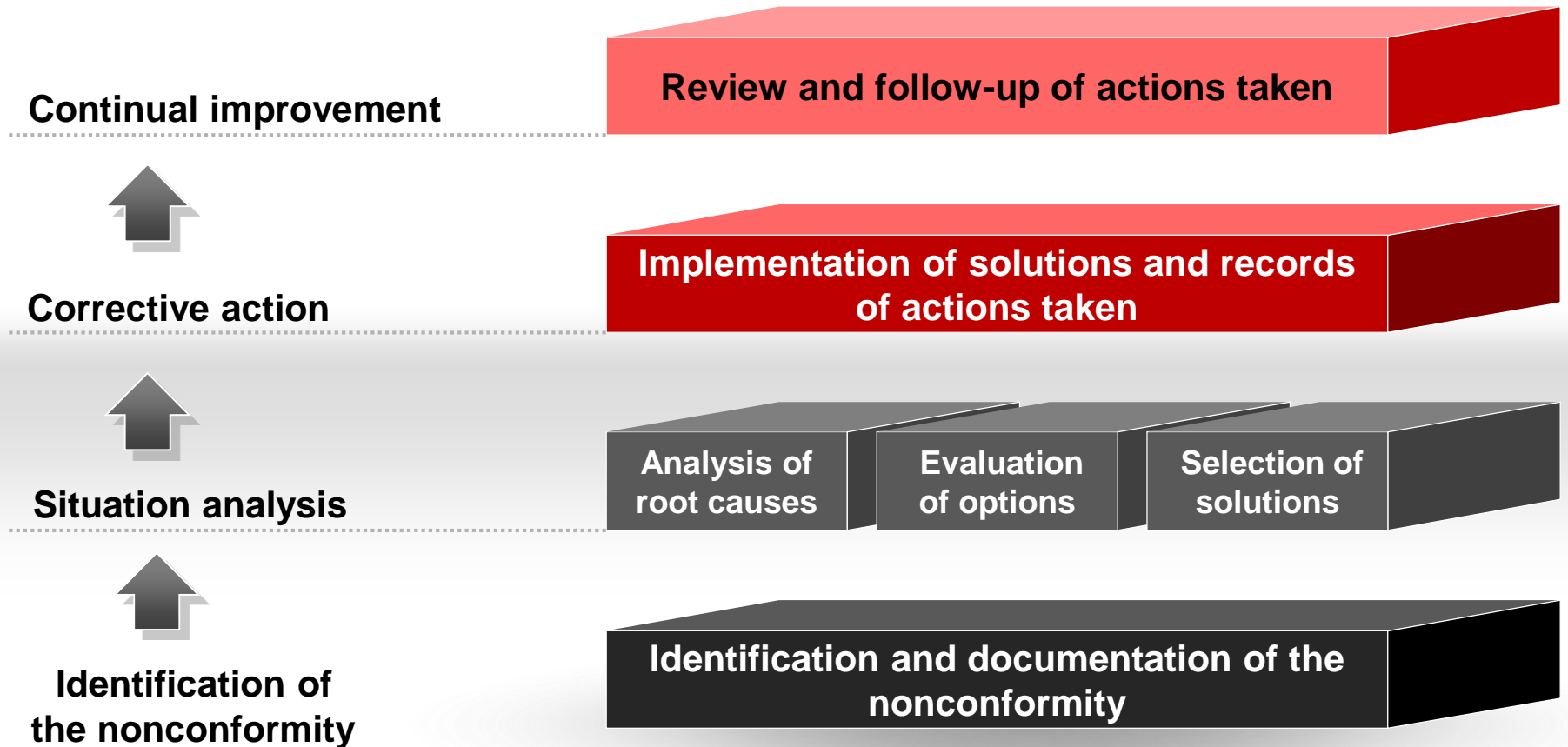
# 4.1. Treatment of non-conformities

## Define a Process to Resolve Problems and Nonconformities



# 4.1. Treatment of non-conformities

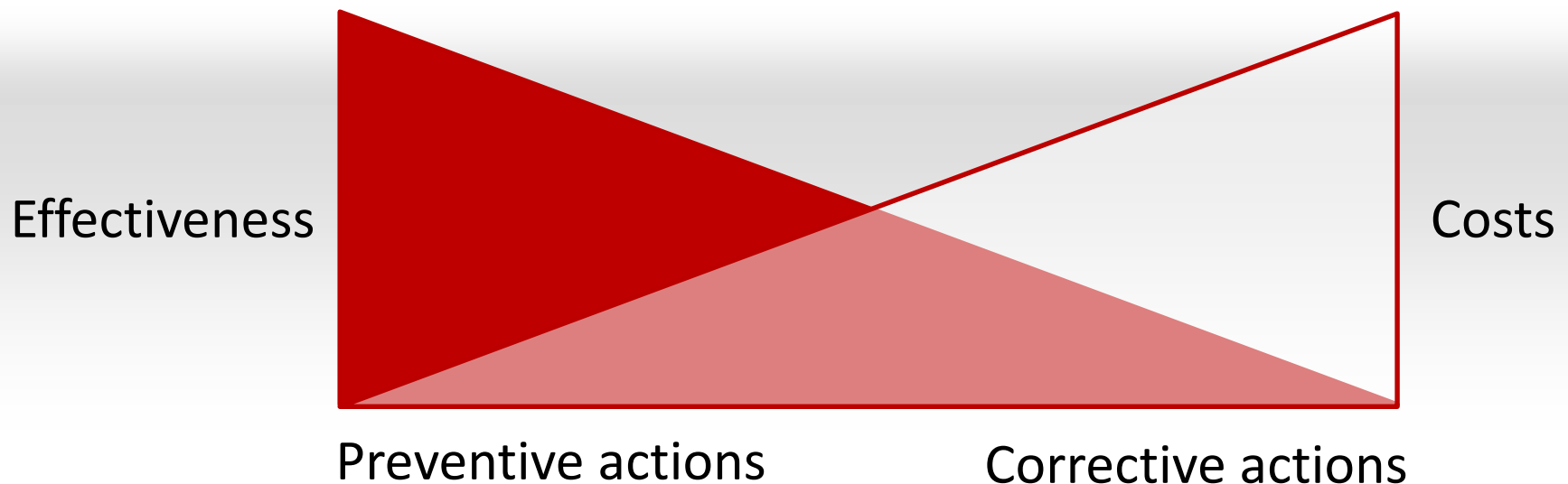
## Corrective Action Procedure



# 4.1. Treatment of non-conformities

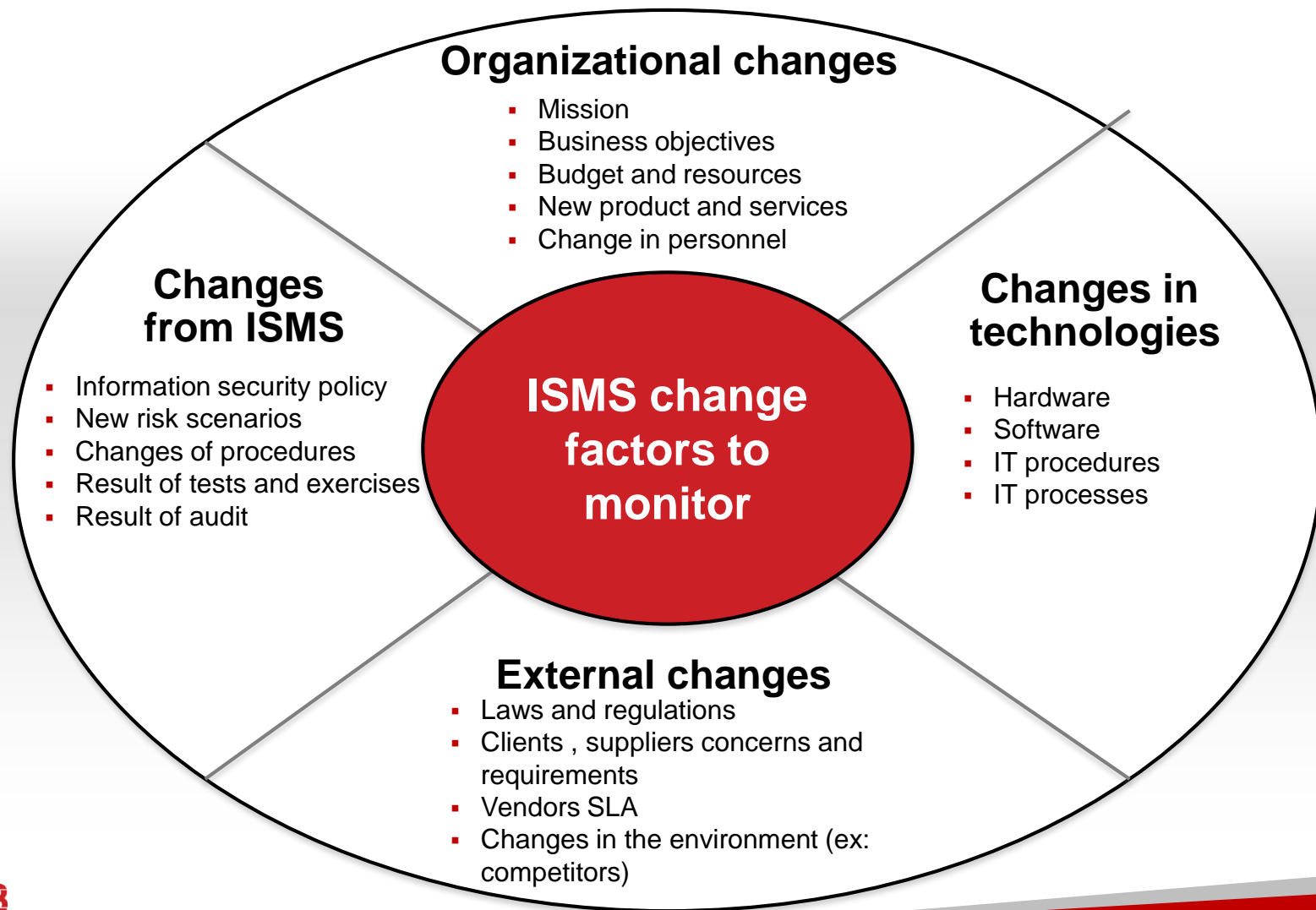
## Preventive Action Procedure

The organization shall determine the actions to **eliminate the potential nonconformity causes** in accordance with the conditions of the ISMS



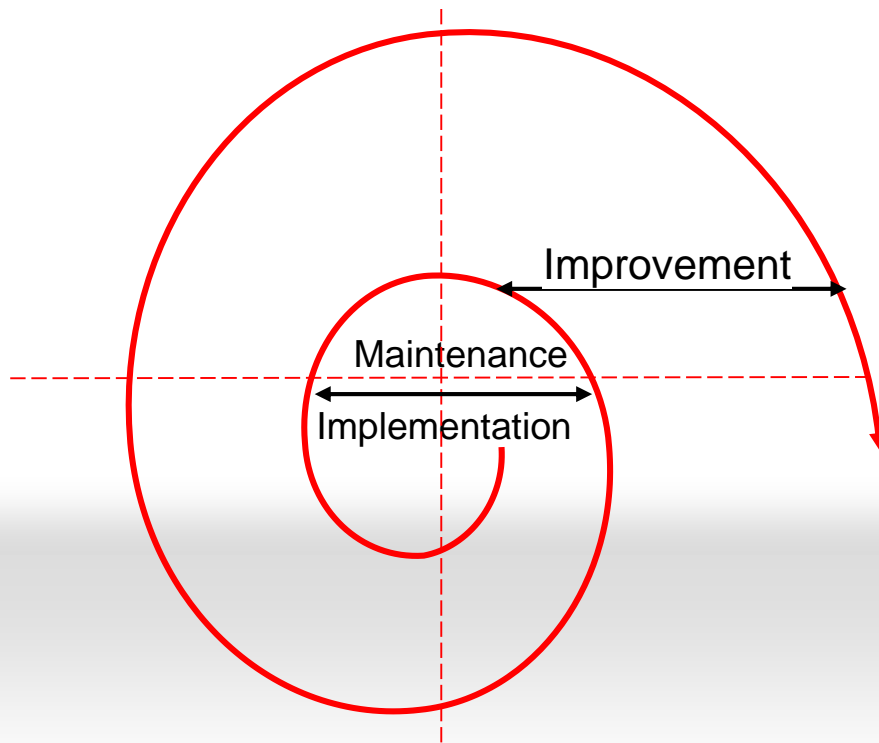
# 4.2. Continual Improvement

## Continuous Monitoring Process of Change Factors



# 4.2. Continual Improvement

## Maintenance and Improvement of the ISMS



- The ISMS needs to be maintained and updated periodically
- Any agreed improvements to the process or actions necessary to improve conformity to the process should be notified to the appropriate managers to have assurance that no risk or risk element is overlooked or underestimated before implementation of changes

# Certification process

## List of activities

