UNIVERSITÉ DU LUXEMBOURG

Incident Management

in the context of an *Information Security Policy*

Master in Information System Security Management

Introduction

To protect its assets (information and systems) on a daily basis an organisation has to:

- **organise** its security by documenting the **countermeasures** or controls to **protect** the **confidentiality**, **integrity** and **availability** of the assets, in a security policy,
- with the prime goal to **manage** and **reduce** its **risks**.

Information Security Policy

→ THE tool for today's (C)ISO ←

Definitions

- **Asset :**
  - anything that has value to the organization.

In the context of **information security**, **two kinds** of assets can be distinguished:

- the **primary** assets:
  - information;
  - business processes and activities;
- the **supporting** assets (on which the primary assets rely), e.g.:
  - hardware;
  - software;
  - network;
  - personnel;

Definitions

- **Control :**
  - **measure** that maintains and/or **modifies** a **risk**

Controls include, but are not limited to, any **process**, **policy**, **device**, **practice** or other conditions and/or actions which maintain and/or modify risk.

NOTE 1: *Controls may not always exert the intended or assumed modifying effect*

NOTE 2: *Control is also used as a synonym for safeguard or countermeasure.*

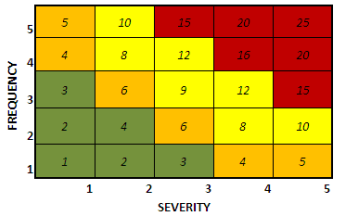
Definitions

- **Process**
  - set of interrelated or **interacting activities** that uses or transforms inputs to deliver a **result**
- **Policy**
  - intentions and direction of an **organization**, as formally expressed by its **top management**
- **Procedure**
  - **specified way** to carry out an activity or a process

Information security policy

- defines the **business rules**, **principles** and standards defining the organisation's approach to managing information security, provides **management direction** and support for information security in accordance with **business requirements** and **relevant laws and regulations**,
- defines **controls** to be implemented to meet the requirements identified by a **risk assessment**,
- needs **approval** by the **highest level of management**.

Sources to start with...



1. One source is derived from assessing risks of the organisation :
   - **Risk = Vulnerability * Threat * Impact**
2. Another source is the ***legal, statutory, regulatory, and contractual requirements*** that an organisation, its trading partners, contractors, and service providers have to satisfy, and their socio- cultural environment.
3. A further source is the particular set of ***principles***, objectives and **business requirements** *for information processing* that an organisation has developed to support its operations.
4. Finally, already ***happened incidents*** and their lessons learned are often a very useful source too.

even before...

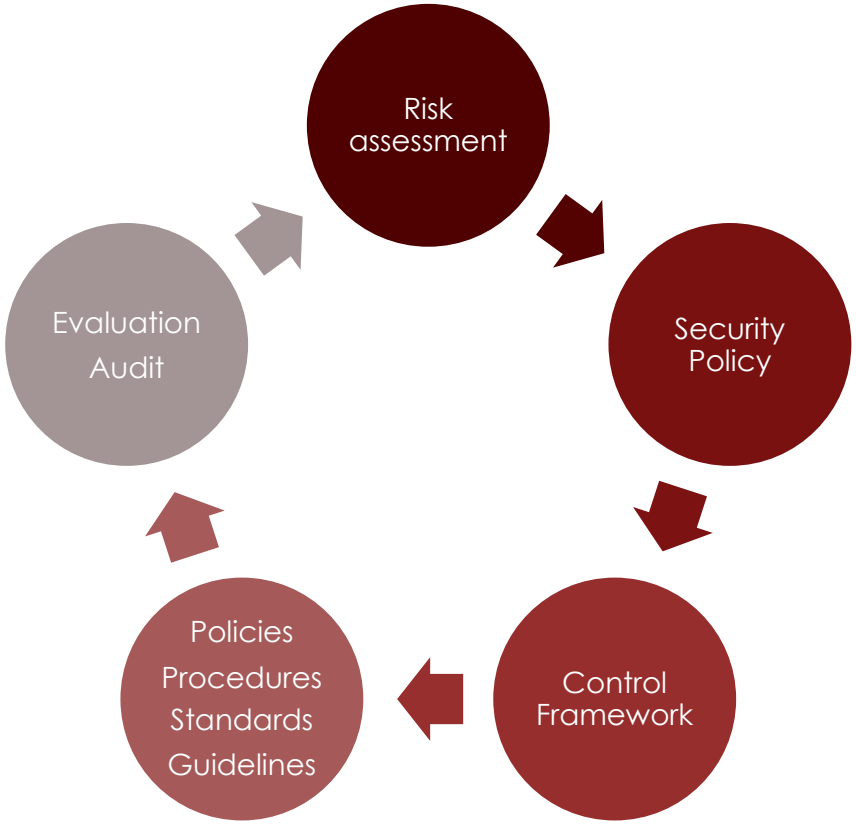
- Before one can identify, quantify, and prioritise risks it is a good practice to identify the organisation's **important/critical assets** on which the risks appose

(→ *asset management/classification*)

Examples are:

- business critical information,
- physical and logical resources (filing cabinet, computers, network equipment, software...),
- staff(most important and critical resources!),
- image, reputation
- know-how, "business" intelligence

Complete *management* lifecycle



ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection – *Information security controls*

formerly known as "Code of practice for information security controls" (2013)

This document provides a **reference set** of generic information security **controls** including implementation **guidance**. This document is designed to be used by organizations:

a) within the context of an information security management system (**ISMS**) based on ISO/IEC 27001;

b) for implementing information security controls based on **internationally recognized best practices**;

c) for developing **organization-specific** information security management **guidelines**.

A **control** is defined as a measure that **modifies or maintains risk**. Some of the controls in this document are controls that modify risk, while others maintain risk. This document provides a generic **mixture** of **organizational**, **people**, **physical** and **technological** information **security controls** derived from internationally recognized best practices.

Life cycle considerations

- **Information** has a life cycle, from **creation to disposal**. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical).
- **Information systems** (and other assets) have life cycles within which they are **conceived, specified, designed, developed, tested, implemented, used, maintained** and eventually retired from service and disposed of.
- **Information security** should be considered at **every stage**.
- **New** system development projects and **changes** to existing systems provide **opportunities to improve** security controls while taking into account the organization's risks and lessons learned from incidents.

ISO 27001:2022

What has changed?

New Name

ISO/IEC 27001:2013

Information technology
– Security techniques
– Information security management systems
– Requirements

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection
– Information security management systems
– Requirements

New relevant requirements – 4.2

ISO/IEC 27001:2013

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

ISO/IEC 27001:2022

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

More focus on processes – 4.4

ISO/IEC 27001:2013

4.4 Information security management system (ISMS)

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

ISO/IEC 27001:2022

4.4 Information security management system (ISMS)

The organization shall establish, implement, maintain and continually improve an information security management system, **including the processes needed and their interactions**, in accordance with the requirements of this document.

New requirements for 6.2

ISO/IEC 27001:2013

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

ISO/IEC 27001:2022

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

New requirements

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

New requirements for 7.4

ISO/IEC 27001:2013

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

~~d) d) who shall communicate; and~~

~~e) the processes by which communication shall be effected.~~

ISO/IEC 27001:2022

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

New requirements for 8.1

ISO/IEC 27001:2013

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

ISO/IEC 27001:2022

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

- **establishing criteria for the processes;**
- **implementing control of the processes in accordance with the criteria.**

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure **that externally provided processes, products or services that are relevant to the information security management system are controlled.**

New requirements for 9.1

ISO/IEC 27001:2013

9.1 Monitoring, measurement, analysis

.....

The organization shall retain appropriate Documented information shall be available documented information as evidence of the as evidence of the results.

ISO/IEC 27001:2022

9.1 Monitoring, measurement, analysis <u>and evaluation</u>

.....

Documented information shall be available documented information as evidence of the as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

New input for management review 9.3

9.3.2 Management review inputs

c) changes in needs and expectations of interested parties that are relevant to the information security management system

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection – *Information security controls*

formerly known as "Code of practice for information security controls" (2013)

This document provides a **reference set** of generic information security **controls** including implementation **guidance**. This document is designed to be used by organizations:

a) within the context of an information security management system (**ISMS**) based on ISO/IEC 27001;

b) for implementing information security controls based on **internationally recognized best practices**;

c) for developing **organization-specific** information security management **guidelines**.

A **control** is defined as a measure that **modifies or maintains risk**. Some of the controls in this document are controls that modify risk, while others maintain risk. This document provides a generic **mixture** of **organizational**, **people**, **physical** and **technological** information **security controls** derived from internationally recognized best practices.

Life cycle considerations

- **Information** has a life cycle, from **creation to disposal**. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical).
- **Information systems** (and other assets) have life cycles within which they are **conceived, specified, designed, developed, tested, implemented, used, maintained** and eventually retired from service and disposed of.
- **Information security** should be considered at **every stage**.
- **New** system development projects and **changes** to existing systems provide **opportunities to improve** security controls while taking into account the organization's risks and lessons learned from incidents.

Overview

Themes *(formerly Clauses)*

The categorization of controls given in Clauses 5 to 8 are referred to as **themes**:

a) **people**, if they concern individual people;

b) **physical**, if they concern physical objects;

c) **technological**, if they concern technology;

d) otherwise they are categorized as **organizational**.

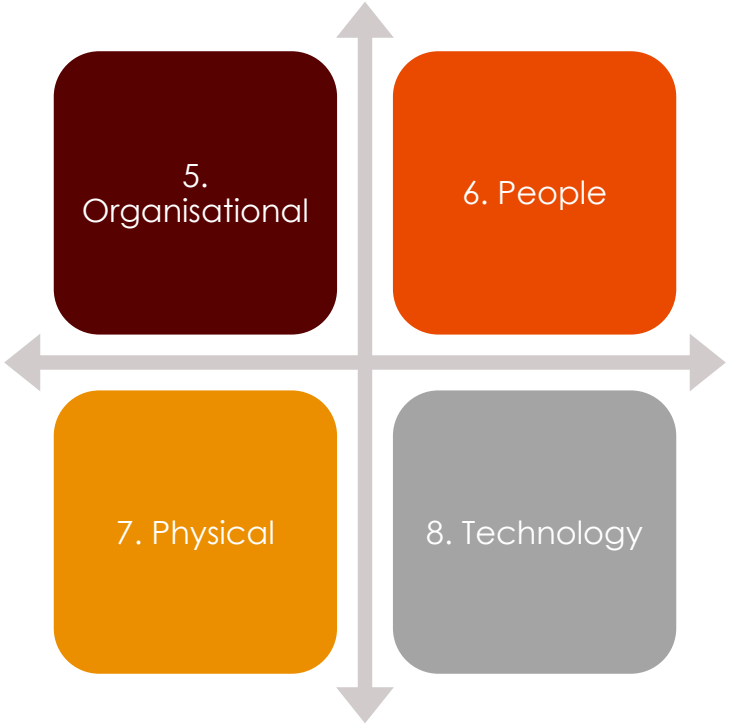
Comparison

2013

114 controls in 14 clauses

2022

93 controls in 4 themes



Overview
Attributes (1)

Each control has been associated with **five attributes** with corresponding attribute values, as follows:

1) **Control type** is an attribute to view controls from the perspective of **when and how** the control modifies the risk with regard to the occurrence of an information security incident.

2) **Information security** properties is an attribute to view controls from the perspective of which **characteristic of information** the control will contribute to preserving.

3) **Cybersecurity concepts** (ref. ISO/IEC TS 27110)

4) **Operational capabilities** is an attribute to view controls from the **practitioner's perspective** of information security capabilities.

5) **Security domains**

Overview
Attributes (2)

1) *Control type* attribute values consist of:
   - **Preventive** (the control that is intended to prevent the occurrence of an information security incident),
   - **Detective** (the control acts when an information security incident occurs) and
   - **Corrective** (the control acts after an information security incident occurs).

2) *Information security properties* attribute values consist of:
   - **Confidentiality**,
   - **Integrity**, and
   - **Availability**.

Overview
Attributes (2)

3) *Cybersecurity concepts* attribute values consist of:
   - **Identify**,
   - **Protect**,
   - **Detect**,
   - **Respond**, and
   - **Recover**.

5) *Security domains* attribute values consist of:
   - **Governance and Ecosystem** includes "Information System Security Governance & Risk Management" and "Ecosystem cybersecurity management" (including internal and external stakeholders);
   - **Protection** includes "IT Security Architecture", "IT Security Administration", "Identity and access management", "IT Security Maintenance" and "Physical and environmental security";
   - **Defence** includes "Detection" and "Computer Security Incident Management";
   - **Resilience** includes "Continuity of operations" and "Crisis management".

Overview
Attributes *(3)*

4) *Operational capabilities* attribute values consist of:
   - **Governance,**
   - **Asset_management,**
   - **Information_protection,**
   - **Human_resource_security,**
   - **Physical_security,**
   - **System_and_network security,**
   - **Application_security,**
   - **Secure_configuration,**
   - **Identity_and_access_management,**
   - **Threat_and_vulnerability_management,**
   - **Continuity,**
   - **Supplier_relationships_security,**
   - **Legal_and compliance,**
   - **Information_security_event_management,** and
   - **Information_security_assurance.**

Overview

*Control **layout***

The layout for each control contains the following:

- **Title** – short name;
- **Attribute table** – A table shows the value(s) of each attribute for the given control;
- **Control** – ***what*** the control is about;
- **Purpose** – ***why*** the control should be implemented;
- **Guidance** – ***how*** the control should be implemented;
- **Other information** – further details, referecnces or related documents

Incident Management

in the context of an Information Security Policy

Organisational controls

- 5.24 Information security incident management planning and preparation
  - Responsibilities and procedures
  - Reporting information security events
  - Reporting security weaknesses
- 5.25 Assessment of information security incidents and decision taking
- 5.5 Contact with authorities
- 5.29 Information security during disruption
- 5.30 ICT readiness for business continuity
- *5.6 Contact with special interest groups*
- *5.7 Threat intelligence*
- *5.26 Information security incident response*
- *5.27 Learning from information security incidents*
- *5.28 Collection of evidence*
- 5.37 Documented operations procedures

CISO

CSIRT/SOC

People, Physical & Technological controls

CISO

- 6.4 Disciplinary process
- 6.8 Information security event reporting
- 7.4 Physical security monitoring

CSIRT/SOC

- 8.13 Information backup
- 8.15 Logging
- 8.16 Monitoring activities

8.8 Management of technical vulnerabilities

Comparison

2013

3 clauses 12 controls

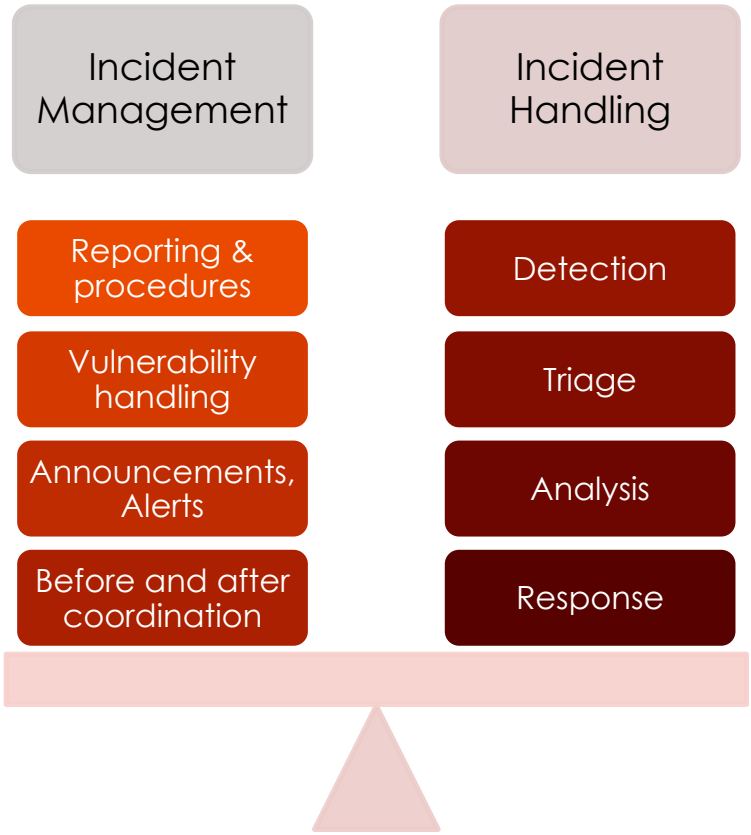
- Clause 16 *(IM)*
  - 7 controls
- Clause 17 *(BC)*
  - 5 controls
- Clause 18 *(C)*
  - 10 controls

2022

3 themes 17 controls

- Theme 5 *(org)*
  - 11 controls
- Theme 6 *(ppl)*
  - 2 controls
- Theme 7 *(phys)*
  - 1 control
- Theme 8 *(tech)*
  - 4 controls

Management *vs.* Handling



Policies & procedures

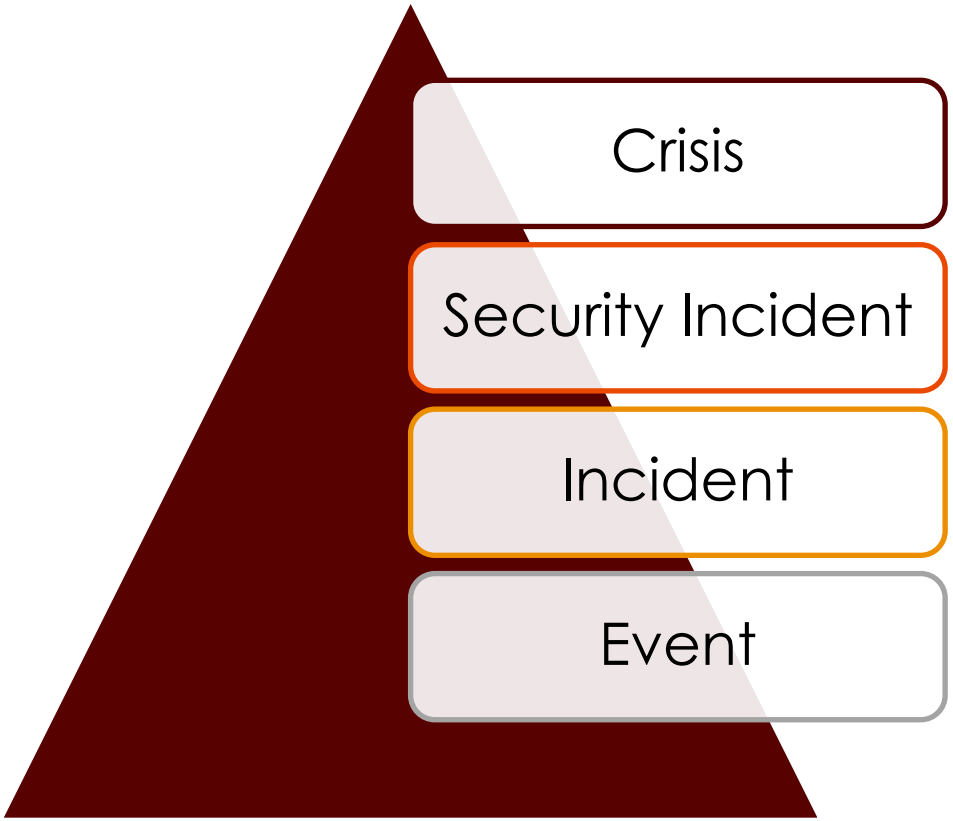
Besides the "security policy", others are important:

- *information classification policy*
- *information disclosure policy*
- *media policy*
- *privacy policy*

Information disclosure TLP (Traffic Light Protocol)

- **TLP:RED** For the eyes and ears of *individual* recipients only, no further disclosure.
- **TLP:AMBER** Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that **TLP:AMBER+STRICT** restricts sharing to the *organization* only.
- **TLP:GREEN** Limited disclosure, recipients can spread this within their community.
- **TLP:CLEAR** Recipients can spread this to the *world*, there is no limit on disclosure.

Pyramid of events (ITU-T E.409)

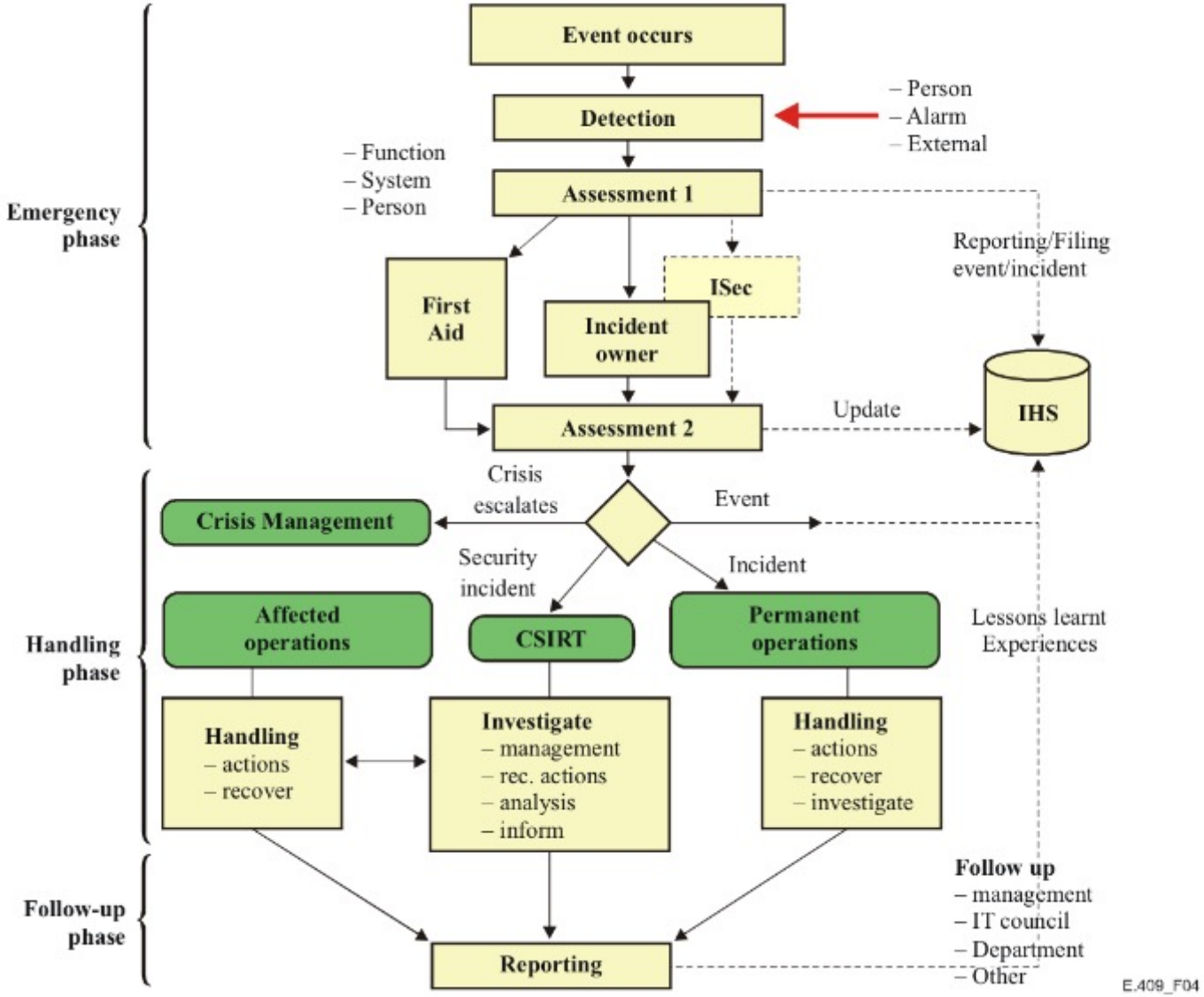


Definitions

- **Event**:
  - An event is an observable occurrence which is not possible to (completely) predict or control.
- **Incident**:
  - An event that might have led to an occurrence or an episode which is not serious.
- **Security incident**:
  - A security incident is any adverse event where by some aspect of security could be threatened.
- **Crisis**:
  - A crisis is a state caused by an event, or the knowledge of a forthcoming event, that may cause severe negative consequences. *During a crisis, one may, in best cases, have the possibility of taking measures to prevent the crisis from becoming a catastrophe. When a catastrophe occurs, a* ***Business Continuity Plan (BCP)*** *shall exist as well as a crisis management team to handle the situation.*

Handling

Following: ITU-T E.409 – Incident organization and security incident handling


Event occurs
Detection
– Person
– Alarm
– External
– Function
– System
– Person
Assessment 1
Emergency phase
First Aid
ISec
Incident owner
Reporting/Filing event/incident
Assessment 2
Update
IHS
Crisis escalates
Event
Crisis Management
Security incident
Incident
Handling phase
Affected operations
CSIRT
Permanent operations
Lessons learnt Experiences
Handling
– actions
– recover
Investigate
– management
– rec. actions
– analysis
– inform
Handling
– actions
– recover
– investigate
Follow-up phase
Follow up
– management
– IT council
– Department
– Other
Reporting
E.409_F04

Roles & Governance

Following: ENISA – Incident Management Guide

Roles

INCIDENT HANDLER	Analyse incidents assigned to him Resolve incidents[22] Fulfil tasks of a duty officer or triage officer if needed Escalate if necessary	Propose improvements in incident handling process Acquire knowledge about new types of incidents
INCIDENT MANAGER	Coordinate daily work of incident handling team; decide how to act in problematic situations Check fulfilment of daily tasks Represent team within the CERT, within the organisation and outside the organisation Advise on how to handle incidents Escalate if necessary	Propose improvements for incident handling team work Discuss balance of incident assignments with incident handlers and triage officers Organise periodic meetings for discussions about incident handling work within team Report to higher management, CISO/CIO, etc
DUTY OFFICER	Ensure that all incidents have owners Be available during service hours	Hand over all remaining work and 'state of the world' to the next duty officer at the end of duty
TRIAGE OFFICER	Check for new incidents Triage incidents in terms of their legitimacy, correctness, constituency origin, severity[21] (constituency/ impact) Hand over incidents to incident handlers in cooperation with the incident manager Report problems with incident	Discuss new kinds of incidents, trends with team members

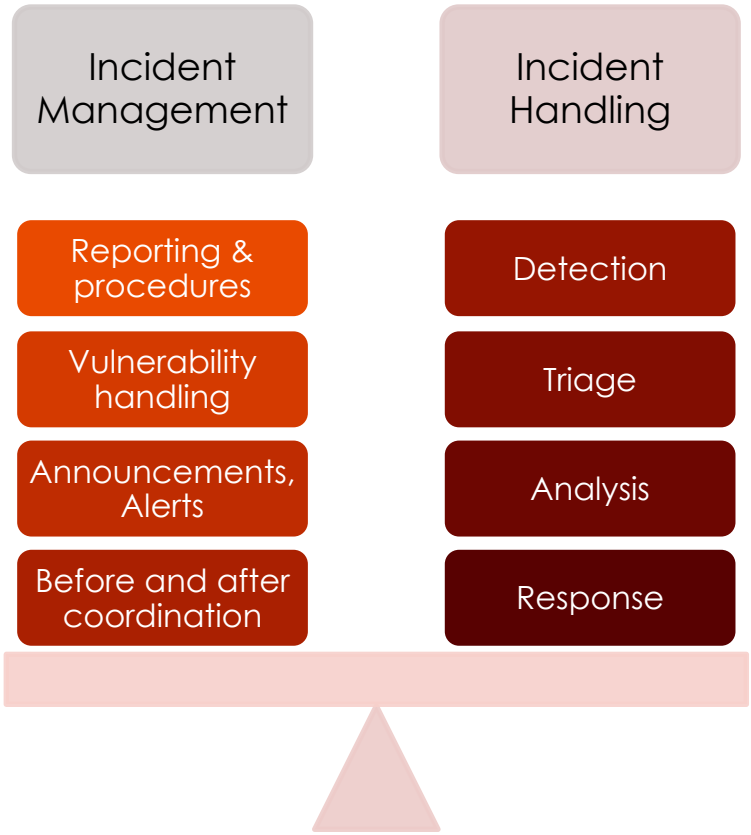
CSIRT

SOC

Governance

- CISO & CIO interactions
  - Prevention and awareness raising
  - Detection and reporting
  - Escalation
- Escalation
  - Clear, well-established mechanism
  - Internal and external considerations
  - Production/operations considerations
- Crisis management
  - Mix of executives, experts, public relations and legal counsels

Management & Handling



Thank you for your attention