
UNIVERSITÉ DU
LUXEMBOURG

UNIVERSITÉ DU LUXEMBOURG

Incident Management

in the context of an Information Security Policy

Management de la Sécurité des Systèmes d'Informations

2

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

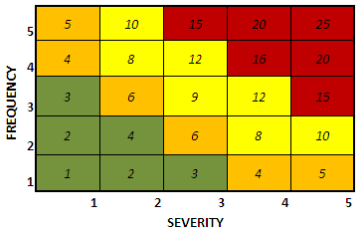
- **Asset :**
  - anything that has value to the organization.
- **Control :**
  - means of **managing risk**, including **policies**, **procedures**, **guidelines**, **practices** or *organizational structures*, which can be of administrative, technical, management, or legal nature.

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

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 **control objectives** and **controls** intended 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...

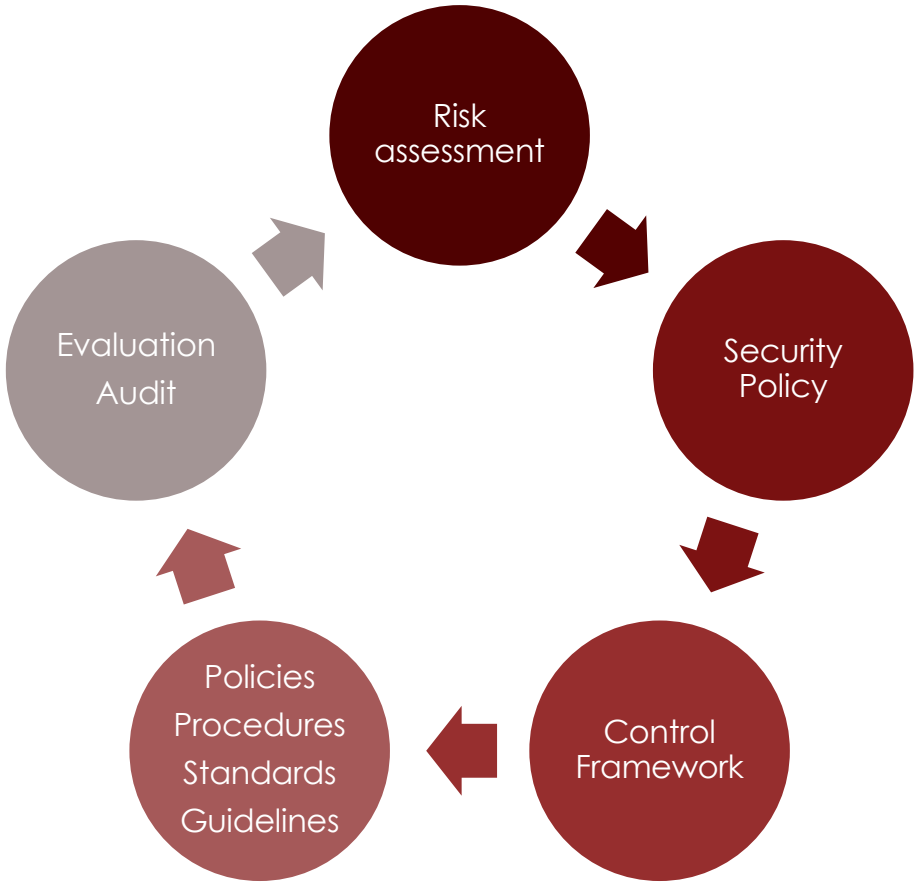
- Before one can identify, quantify, and prioritise risks it is a good practice to identify the organisation's **important/critical assets** on which the risks appose

(→ *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 27002:2013

"Code of practice for information security controls"
(formerly known as ISO/IEC 17799 and BS7799)

Scope

- "This International Standard gives **guidelines for organizational** information security **standards** and information security **management practices** including the selection, implementation and management of **controls** taking into **consideration** the organization's information security **risk environment(s)**."
- "The International Standard is designed to be used by organizations that intend to:
  - select controls within the process of implementing an **Information Security Management** System based on **ISO/IEC 27001** ;
  - implement **commonly accepted** information security controls ;
  - develop their **own** information security management **guidelines**.

Overview

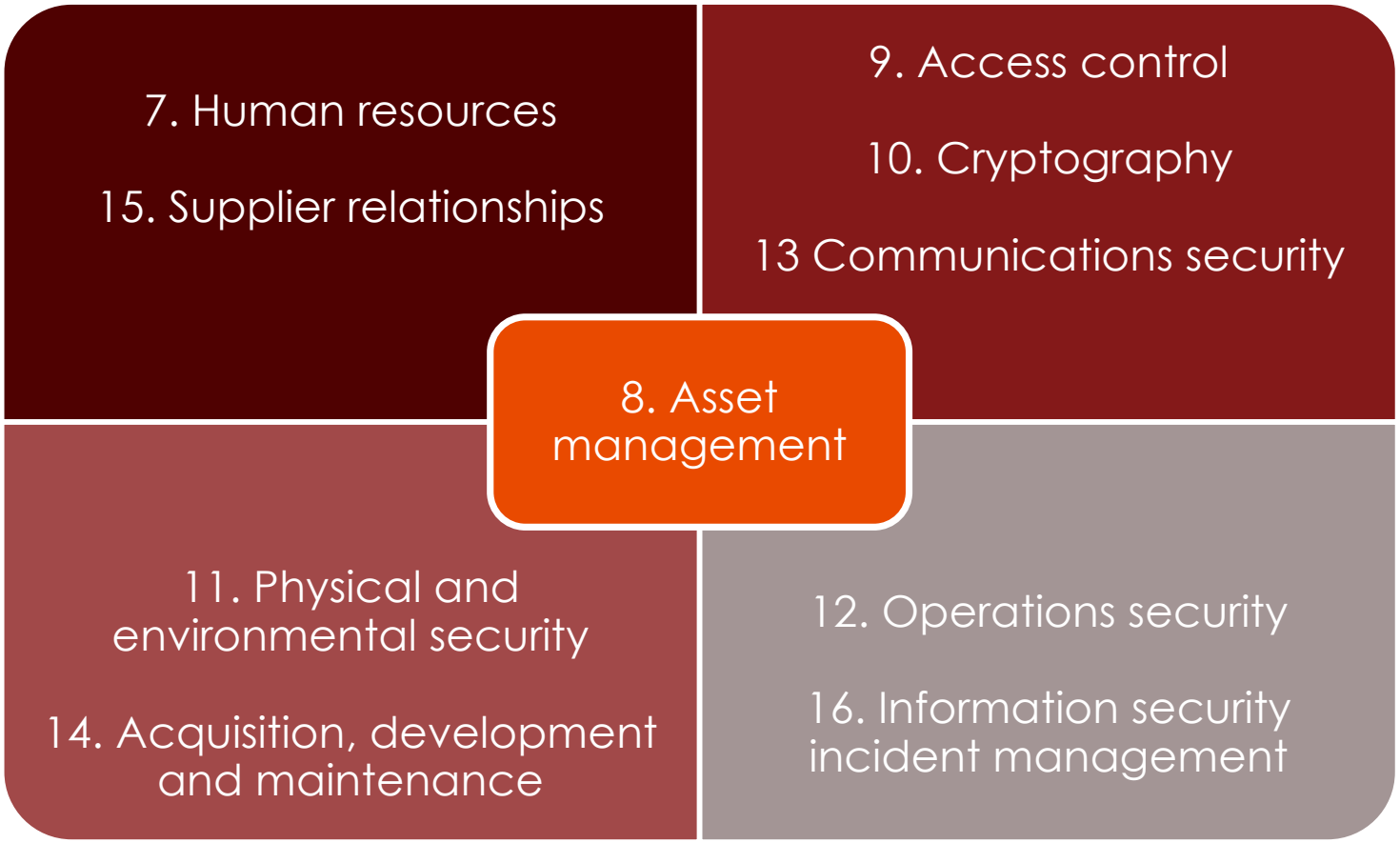
5. & 6. information security policy & organisation

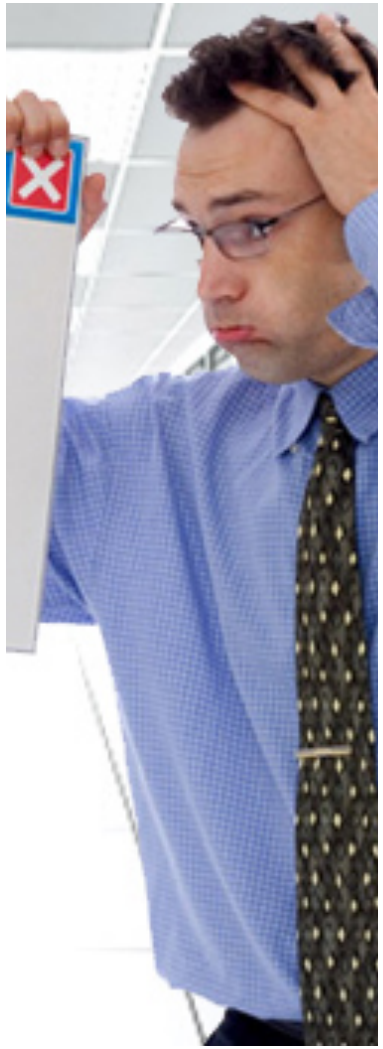
18. Compliance

17. Business continuity management

- 7. Human resources
- 15. Supplier relationships
- 9. Access control
- 10. Cryptography
- 13 Communications security
- 8. Asset management
- 11. Physical and environmental security
- 14. Acquisition, development and maintenance
- 12. Operations security
- 16. Information security incident management

Core clauses





Clause 16
Incident management

- Responsibilities and procedures
- Reporting information security events
- Reporting security weaknesses
- Appreciation of information security incidents and decision taking
- Information security incident response
- Learning from information security incidents
- Collection of evidence

Clause 17
Business continuity

- Including information security in the business continuity management process
- Business continuity planning framework
- Developing and implementing continuity plans including information security
- Testing, maintaining and re-assessing business continuity plans
- Redundancy and availability of information systems

Clause 18 Compliance

- Compliance with legal requirements
  - Identification of applicable legislation
  - Intellectual property rights (IPR)
  - Protection of organizational records
  - Data protection and privacy of personal information
  - Regulation of cryptographic controls
- Information security audit considerations
  - Independent Information systems audit
  - Compliance with security policies and standards
  - Technical compliance checking

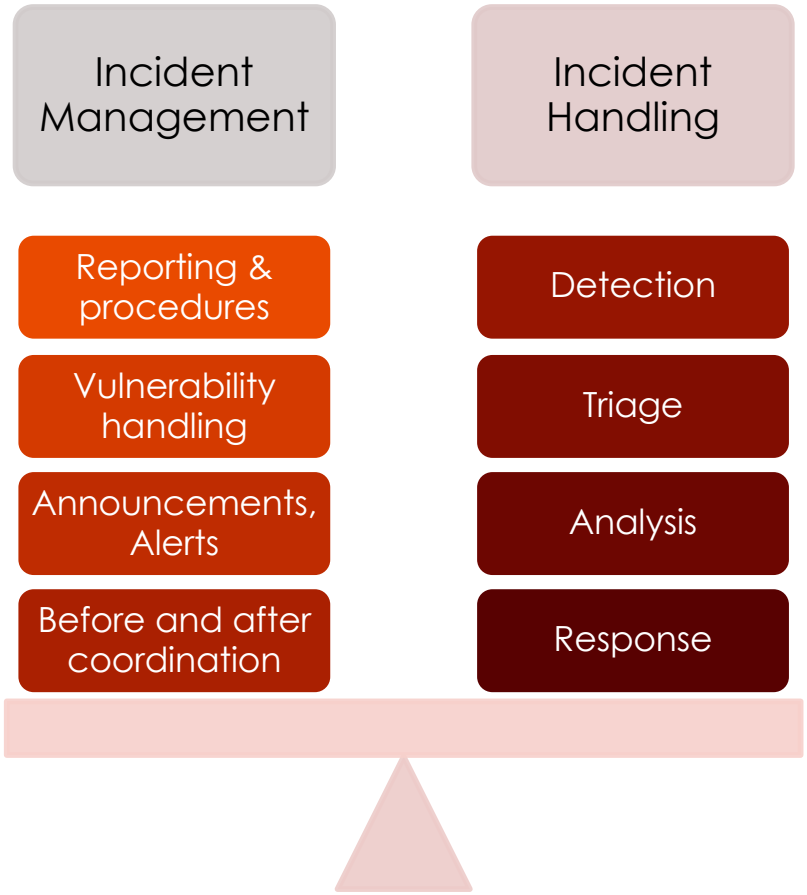
Management of information security incidents (clause 16)

- Responsibilities and procedures
- Reporting information security events
- Reporting security weaknesses
- Assessment of information security incidents and decision taking
  - *Information security incident response*
  - *Learning from information security incidents*
  - *Collection of evidence*

CISO

CSIRT | CERT | SOC

Management *vs.* Handling



Policies & procedures

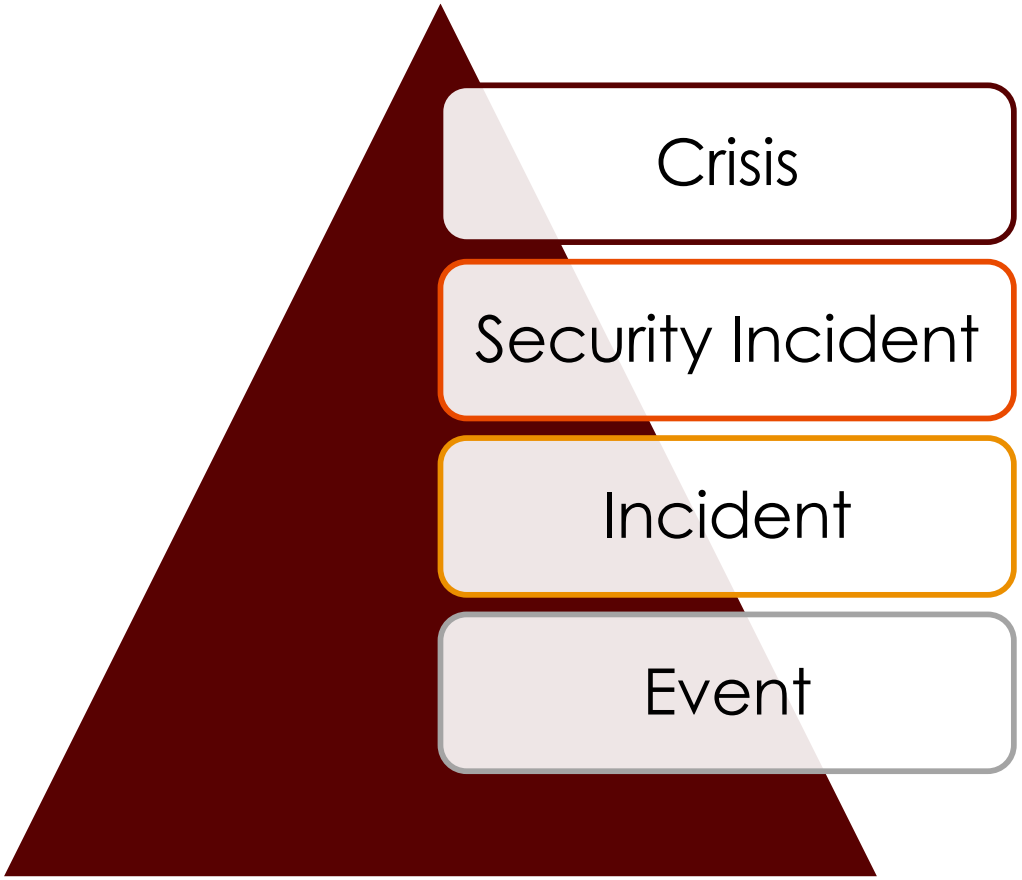
Besides the "security policy", others are important:

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

Information disclosure
TLP (Traffic Light Protocol)

RED	Non-disclosable information and restricted to representatives participating in the information exchange themselves only. Representatives must not disseminate the information outside the exchange. RED information may be discussed during an exchange, where all representatives participating have signed up to these rules. Guests and others such as visiting speakers who are not full members of the exchange will be required to leave before such information is discussed.
AMBER	Limited disclosure and restricted to members of the information exchange; those within their organisations and/or constituencies (whether direct employees, consultants, contractors or outsource-staff working in the organisation) who have a NEED TO KNOW in order to take action.
GREEN	Information can be shared with other organisations, information exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web.
WHITE	Information that is for public, unrestricted dissemination, publication, web-posting or broadcasting. Any member of the information exchange may publish the information, subject to copyright.

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.*

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	Co[illegible] 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

CSIRT/CERT

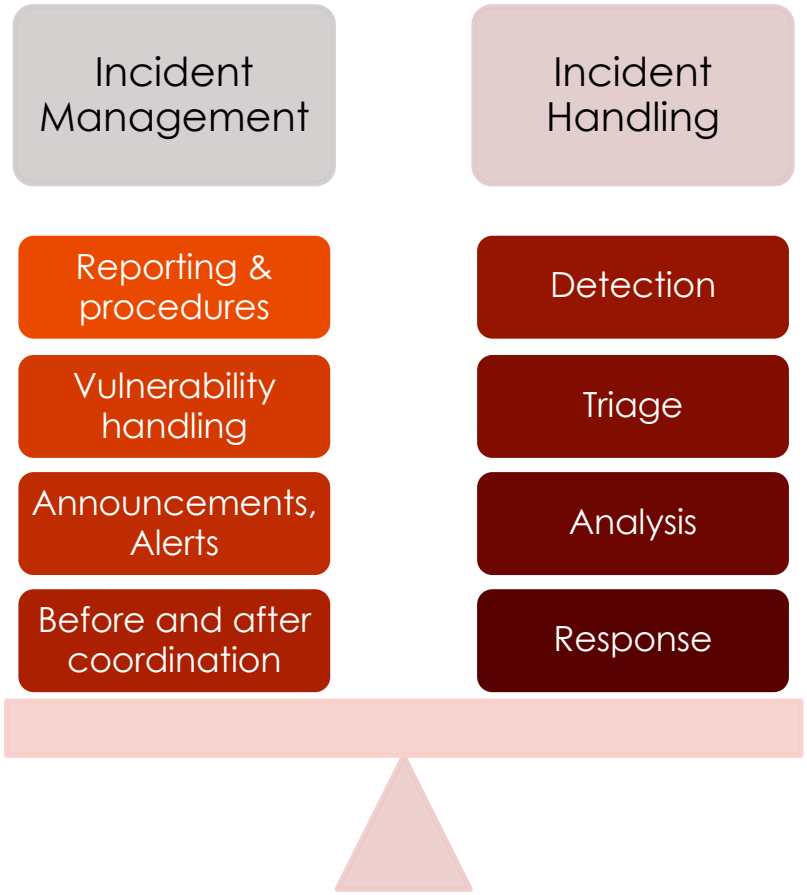
DUTY OFFICER	Ensure that all incidents have owners Be available during service hours	Hand over all remaining work and 'state of the world' to the next duty officer at the end of duty
TRIAGE OFFICER	Check for new incidents [illegible]idents in terms of their legitimacy, correctness, constituency origin, 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

SOC

Governance

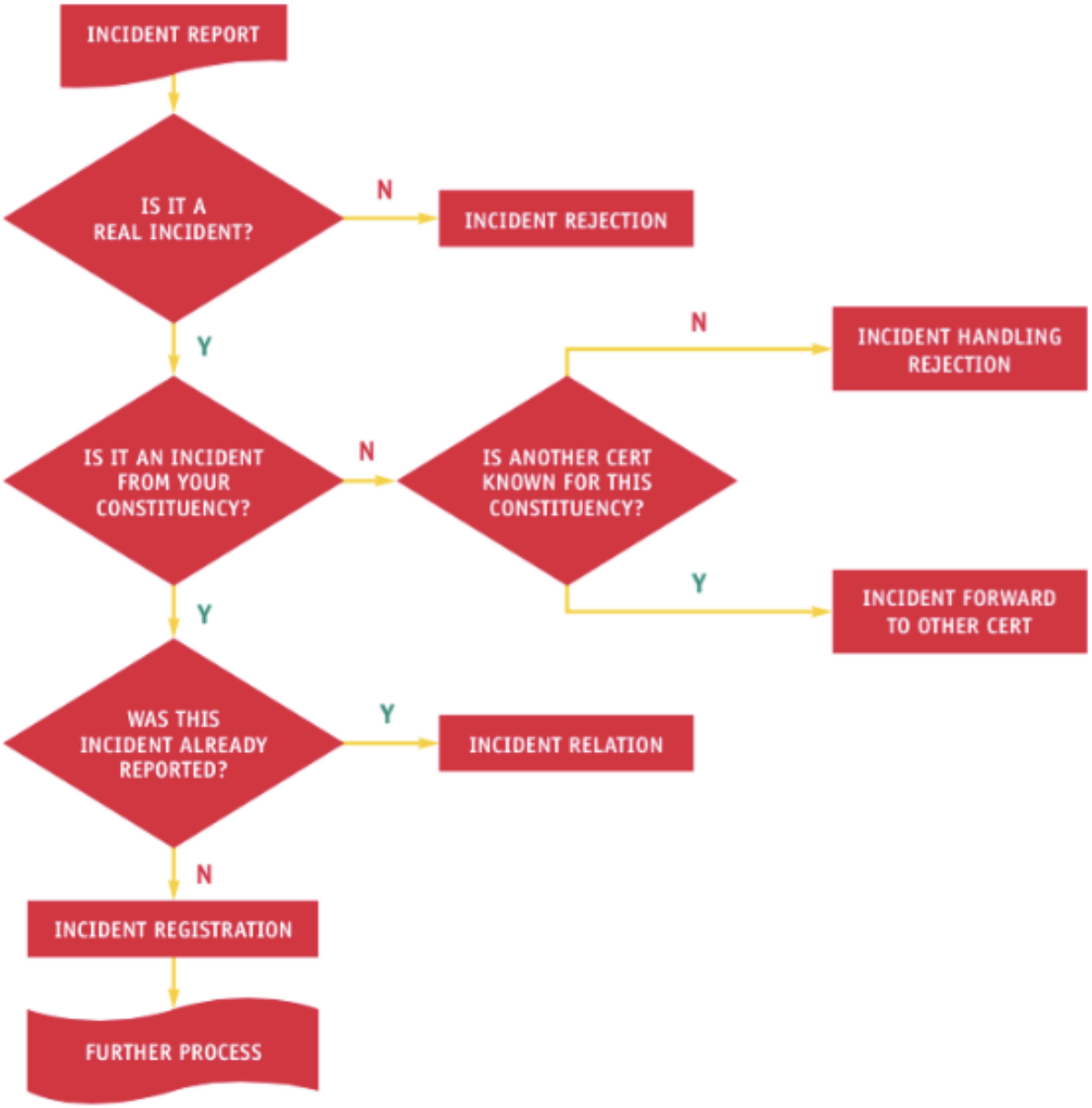
- CISO & CIO interactions
  - Prevention and awareness raising
  - Detection and reporting
  - Escalation
- Escalation
  - Clear, well-established mechanism
  - Internal and external considerations
  - Production/operations considerations
- Crisis management
  - Mix of executives, experts, public relations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

Management & Handling



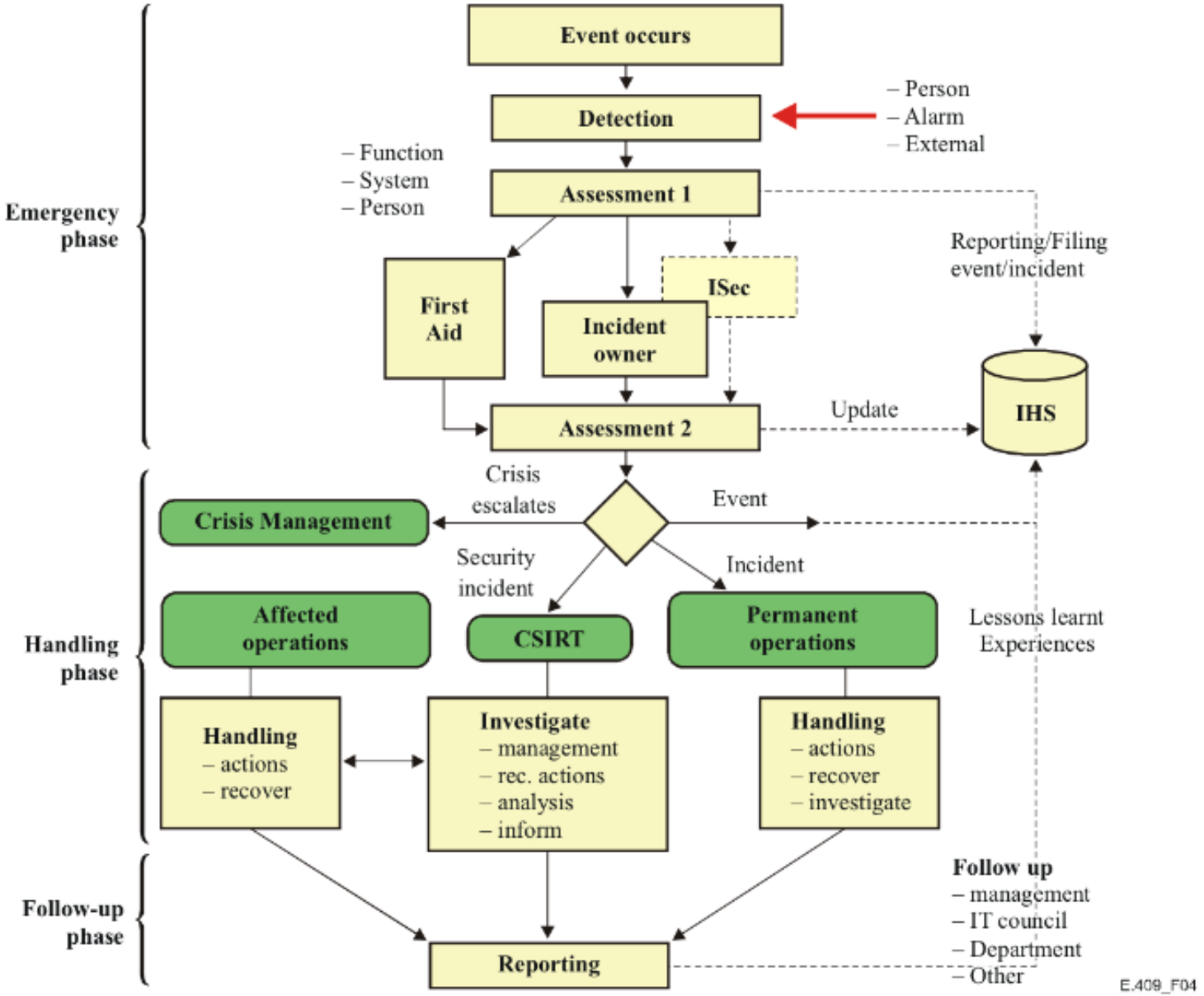
Reporting

Following: ENISA – Incident Management Guide


INCIDENT REPORT
IS IT A REAL INCIDENT?
N
INCIDENT REJECTION
Y
IS IT AN INCIDENT FROM YOUR CONSTITUENCY?
N
IS ANOTHER CERT KNOWN FOR THIS CONSTITUENCY?
N
INCIDENT HANDLING REJECTION
Y
INCIDENT FORWARD TO OTHER CERT
Y
WAS THIS INCIDENT ALREADY REPORTED?
Y
INCIDENT RELATION
N
INCIDENT REGISTRATION
FURTHER PROCESS

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
IHS
Update
Assessment 2
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


UNIVERSITÉ DU
LUXEMBOURG