NRD Cyber Security

ISO 27035 practical value for CSIRTs and SOCs

Vilius Benetis

https://www.linkedin.com/in/viliusbenetis/

NRD Cyber Security

FOCUS

Cybersecurity operations build-out, incident detection and handling, establishment and support of Computer Security Incident Response Teams (CSIRTs), and cyber capacity enhancement at organisational and national levels.

CUSTOMERS

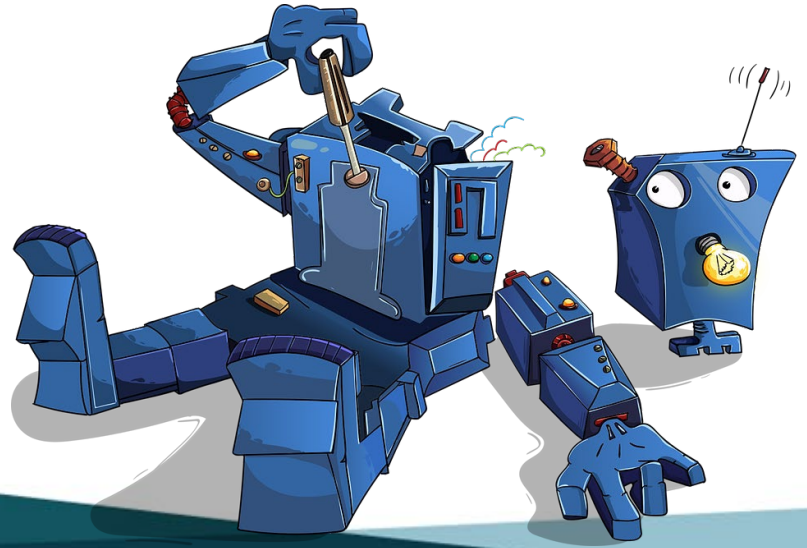
Governments, public and private sector organisations.

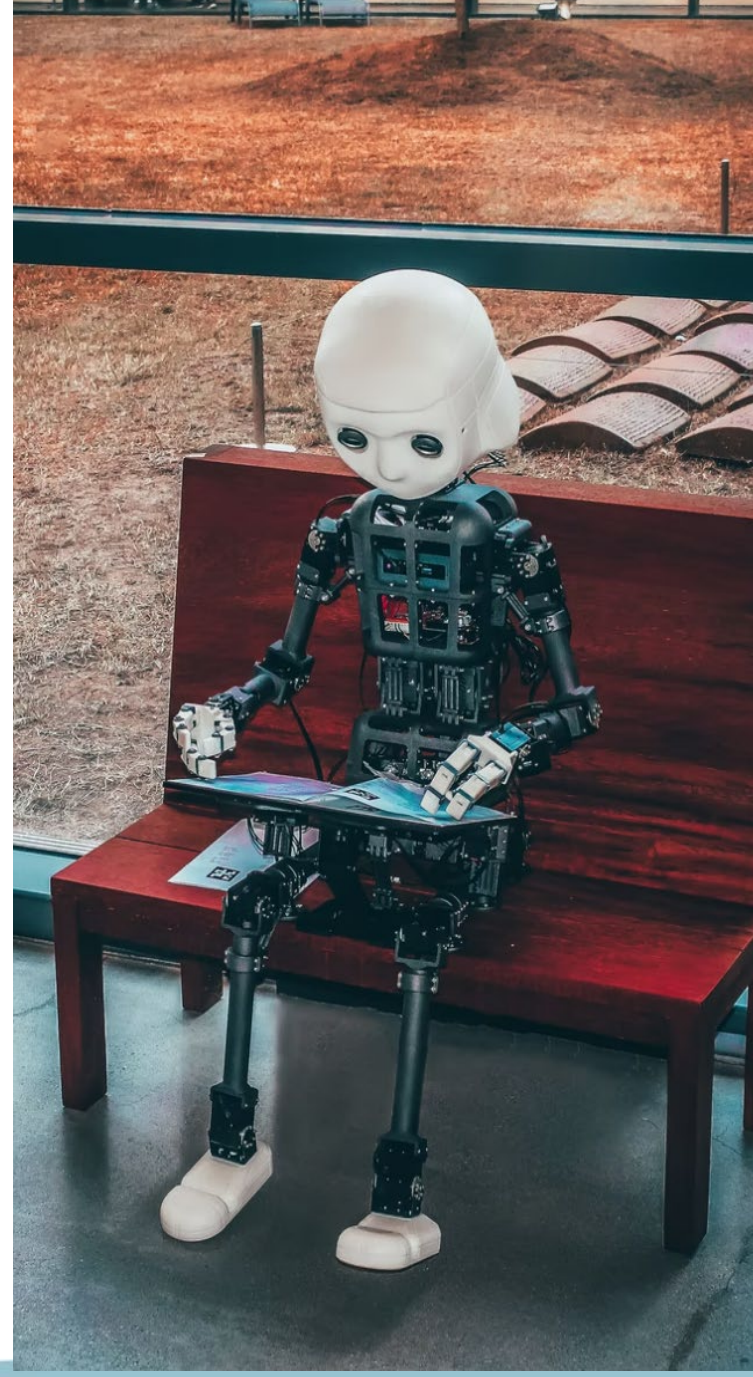
Modernization of CSIRTs and SOCs

- **CSIRTs and SOCs are increasingly expected to work as professional and effective organizations**
  - which can reflect on own performance and improvement.

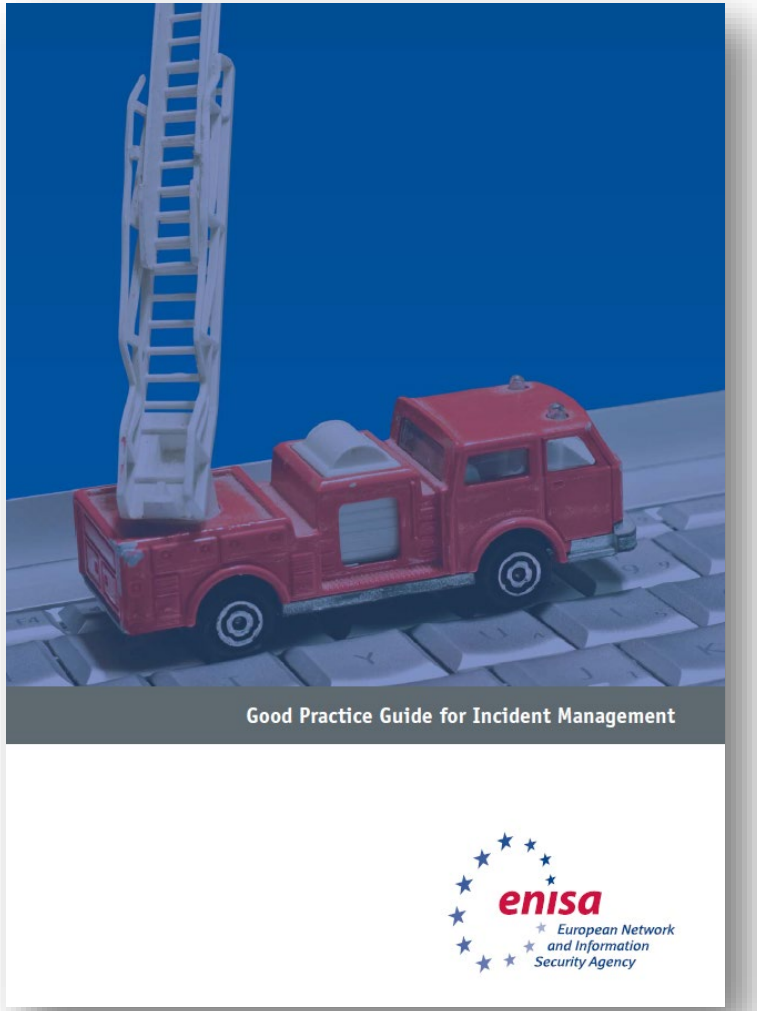
- **Such expectation is quite a challenge for many teams around the world.**

How ISO 27035 would be of help here?





Common methodologies used for Infosec Incident Management



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

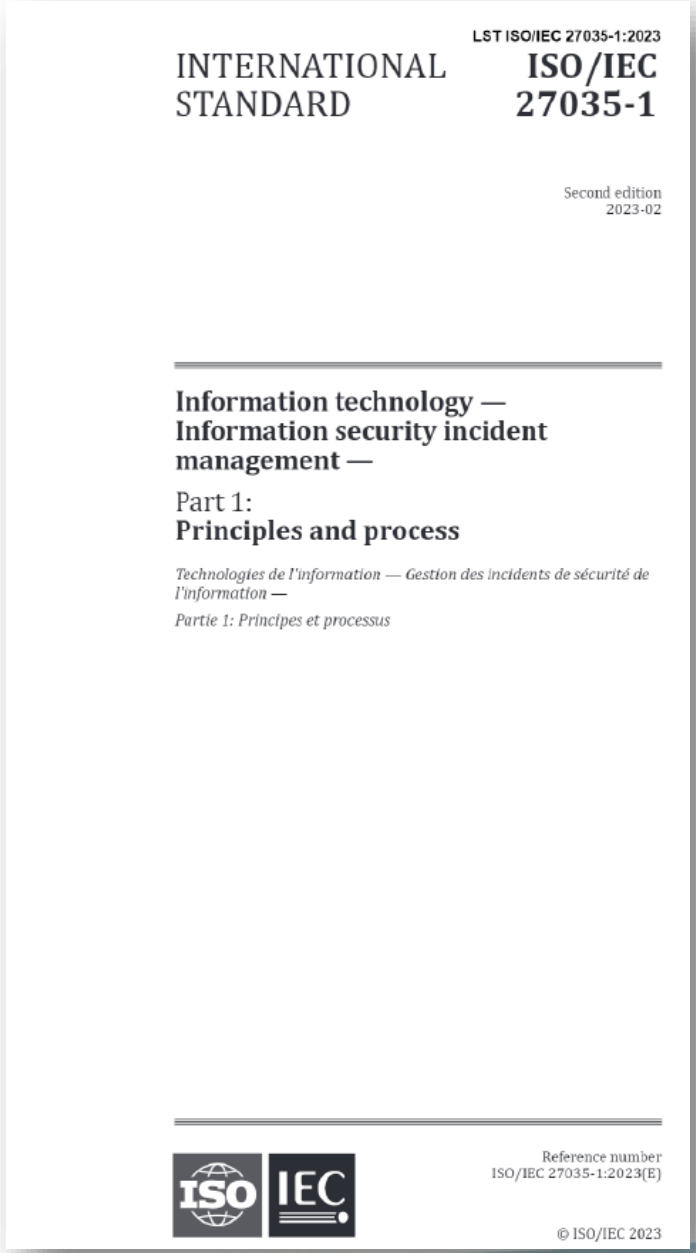
Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

About:

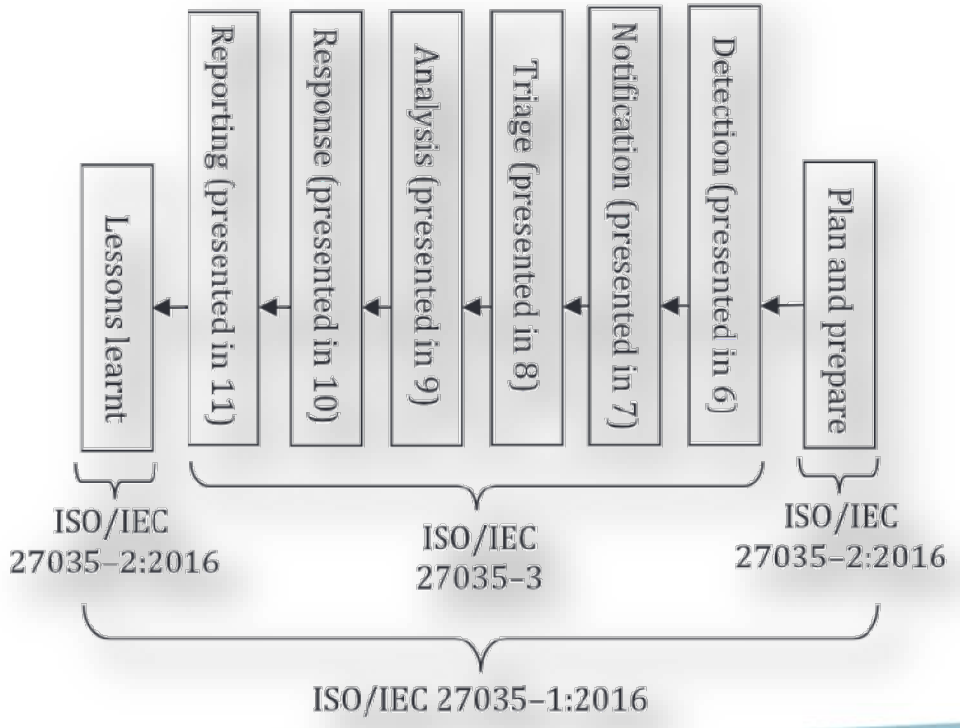
1. Understanding ISO 27035
2. Positioning ISO 27035 at CSIRT/SOC
3. Applicability of ISO 27035: usage, content



ISO 27035 Information technology — Information security incident management (IT-ISIM)

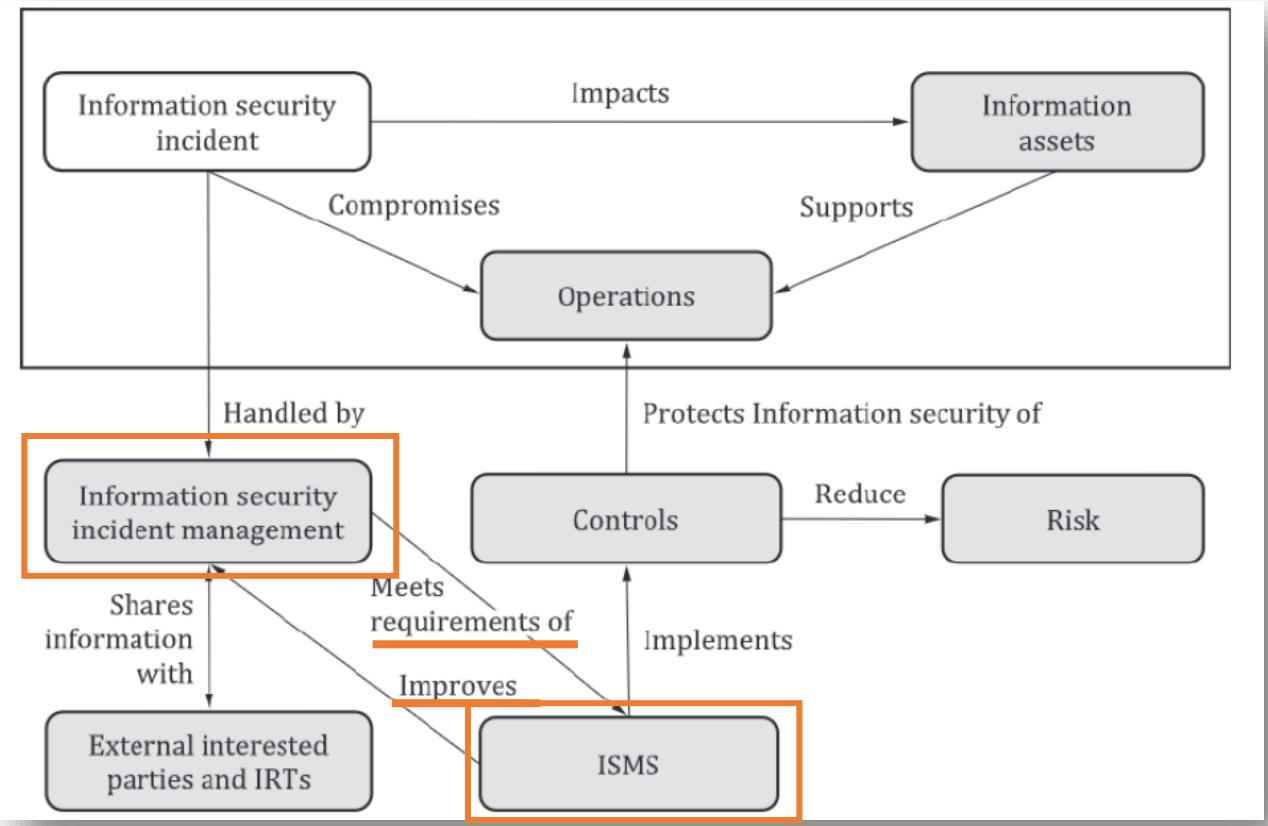
- 27035-1 Part1: **Principles and process** / 2023-02 (2nd ed., 33p.)
- 27035-2 Part2: **Guidelines to plan and prepare for incident response** / 2023-02 (2nd ed., 53p.)
- 27035-3 Part3: **Guidelines for ICT incident response operations** / 2020-09 (1st ed., 31p.)
- 27035-4 Part4: **Coordination** / Not released yet (CD stage?, 22p.)

Cost: iso.org: **640 CAD**, lsd.lt: **200 CAD**
In some country maybe it is free…



Reason to exist

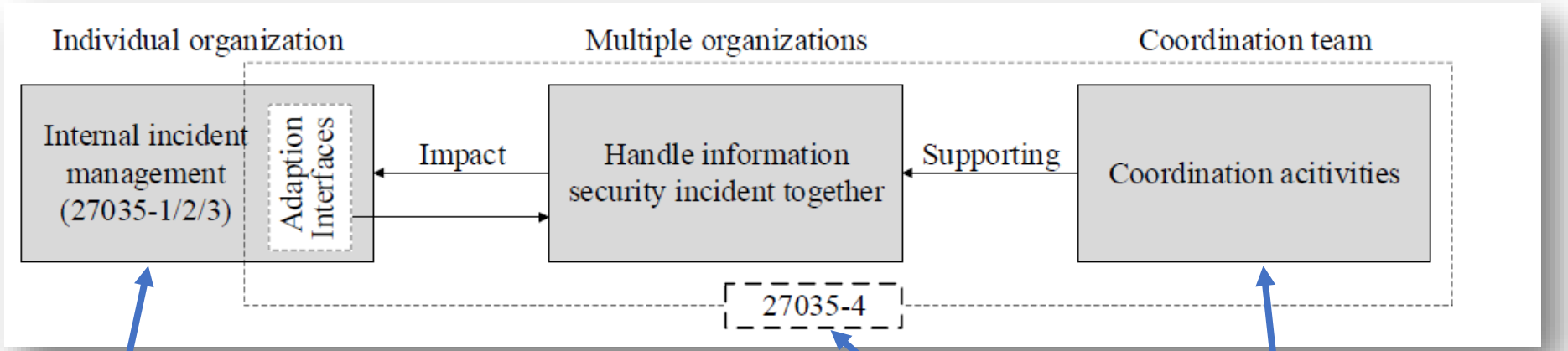
- To support 27001/27002 by providing more detail InfoSec Incident management controls guidance, adjusted to own risk
  - The I27035 series is not a comprehensive guide!



Supports 27001 Annex A:

5.24 Infosec incident mng planning and preparation
5.25 Assessment and decision on infosec Events
5.26 Response to infosec incidents
5.27 Learning from infosec incidents
5.28 Collection of evidence
6.8 Information security event reporting

Application for CSIRT/SOCs:



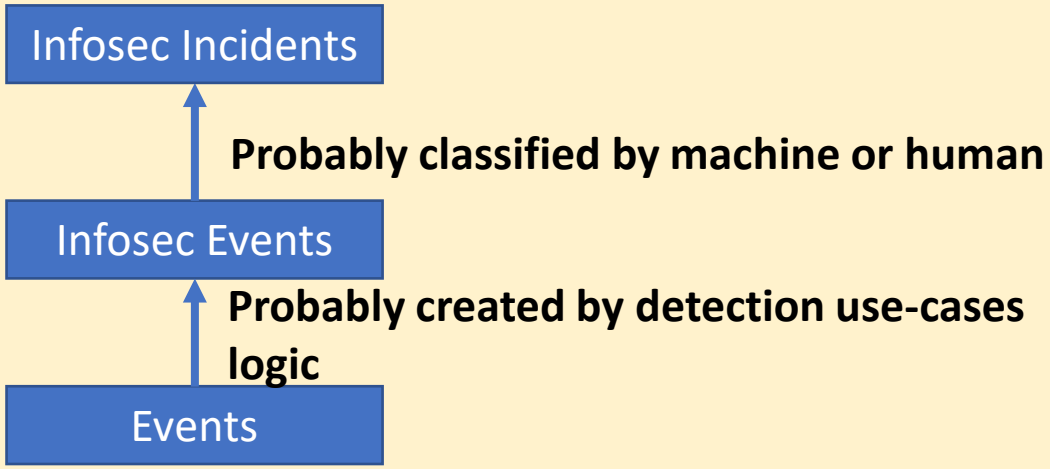
Internal SOCs, CSIRTs, MSSPs

Promote

National, Sector CSIRTs, SOCs, ISACs

Worldviews

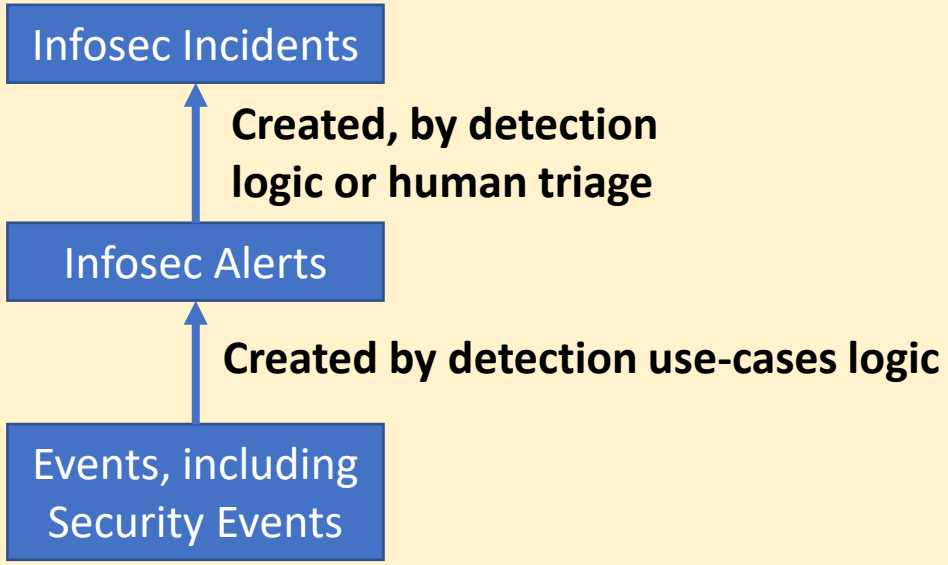
ISO 27035 World



Infosec event - indicates a
1) possible breach of infosec or
2) failure of controls

Infosec incident – Infosec events with risk of harm an organization (assets, operations)

My World



SIEM, SOAR, EDR, MDR, XDR, SOC, CSIRT

ISO 27035 Model

- **Infosec incident management** – handling infosec incidents in consistent way
  - **Incident handling** –
    detecting / reporting / assessing / responding / dealing with / learning from infosec incidents
  - **Infosec investigation** - examinations, **analysis** and interpretation to understand of an Infosec incident
  - **incident response –** mitigation / resolution infosec incidents, including to protect and restore

- **incident management team** (IMT), lead by **Incident Manager**, for all infosec incident management activities throughout the incident (handling?) lifecycle (-2: manager should be close to CxOs, might handle SOC area)

- **incident response team** (IRT), lead by **Incident Coordinator,** for responding to and resolving incidents in a coordinated way. Can be a few in a big organization.

Causes for Infosec Events and Incidents

1. Humans make errors
2. Technology fail
3. Vulnerabilities due to imperfection of controls
4. Risk - assessment: incomplete, - treatment: not cover risks; - changes in the context

Objectives of infosec incident management

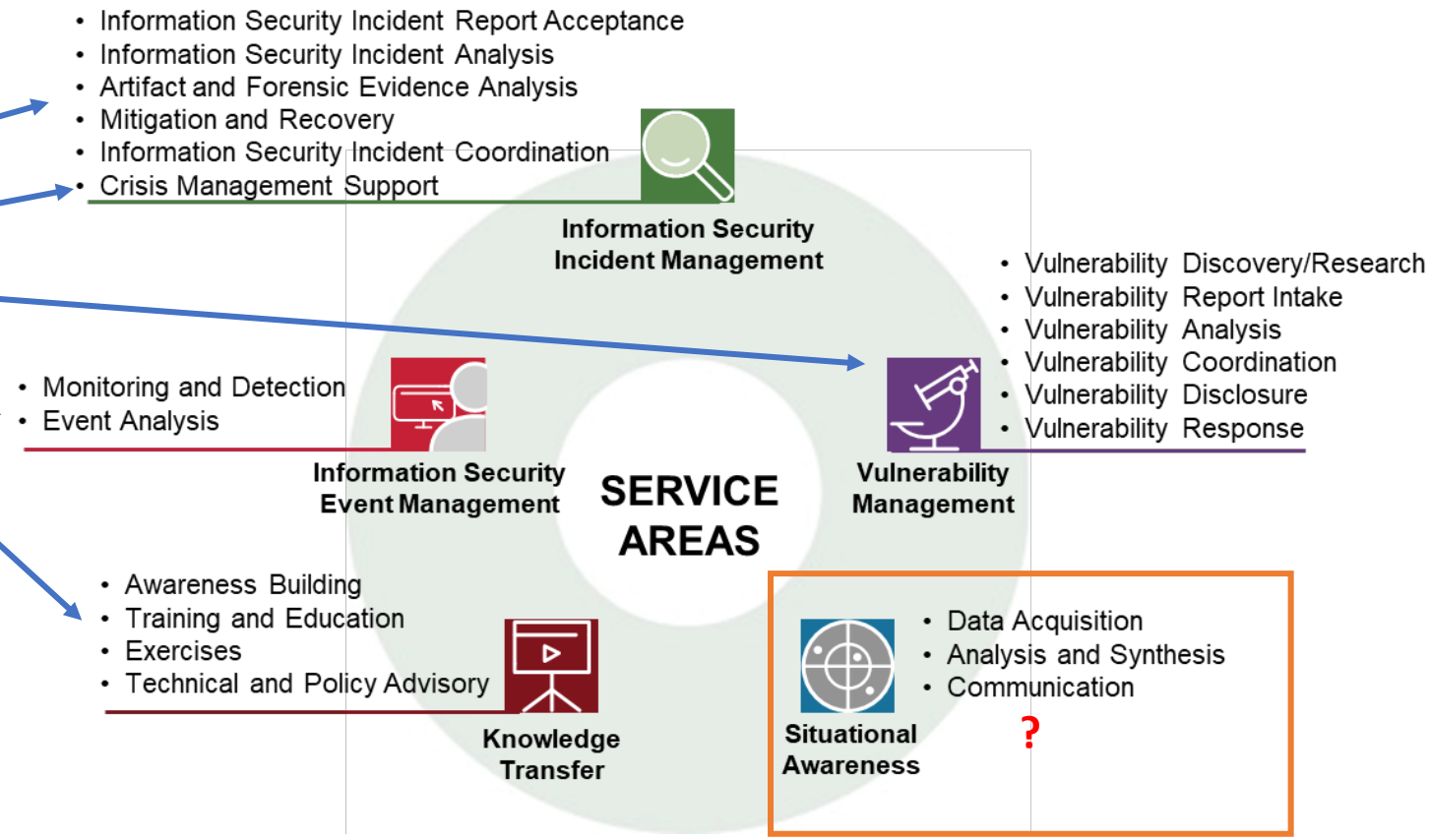
1. **Infosec events** are detected, dealt with, incl. classified as infosec incidents
2. **Infosec incidents** are assessed and responded effectively (process, time)
3. **Adverse impact** of infosec incidents are minimized by appropriate controls as part of **incident response**
4. Link with **crisis management** and **BCP** through an escalation process is established.
5. **Infosec vulnerabilities** during the incident are assessed / dealt - to prevent or reduce incidents.
6. **Lessons are learnt quickly** from infosec incidents, related vulnerabilities and their management.

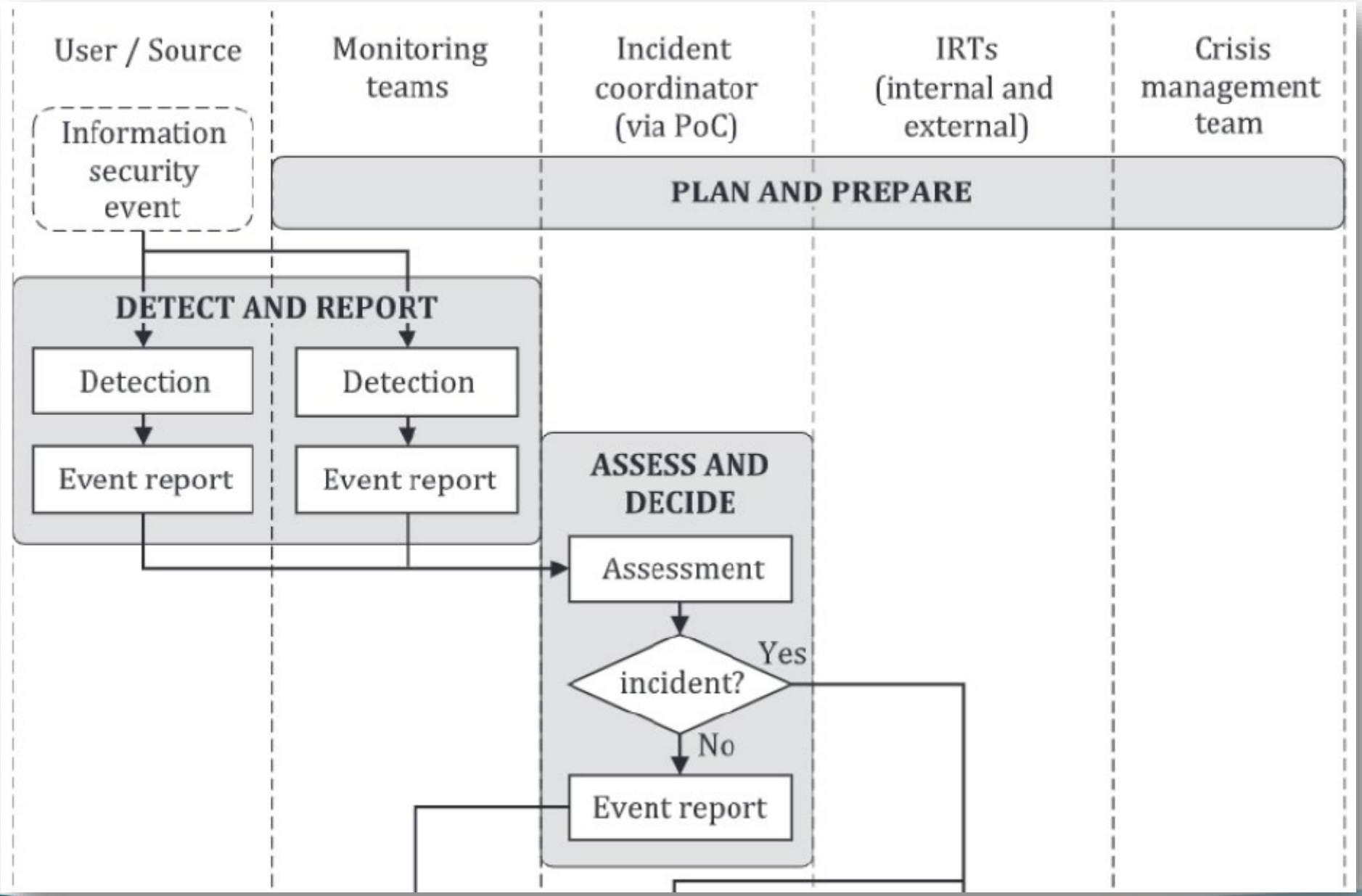
Benefits of structuring Infosec Incident Management

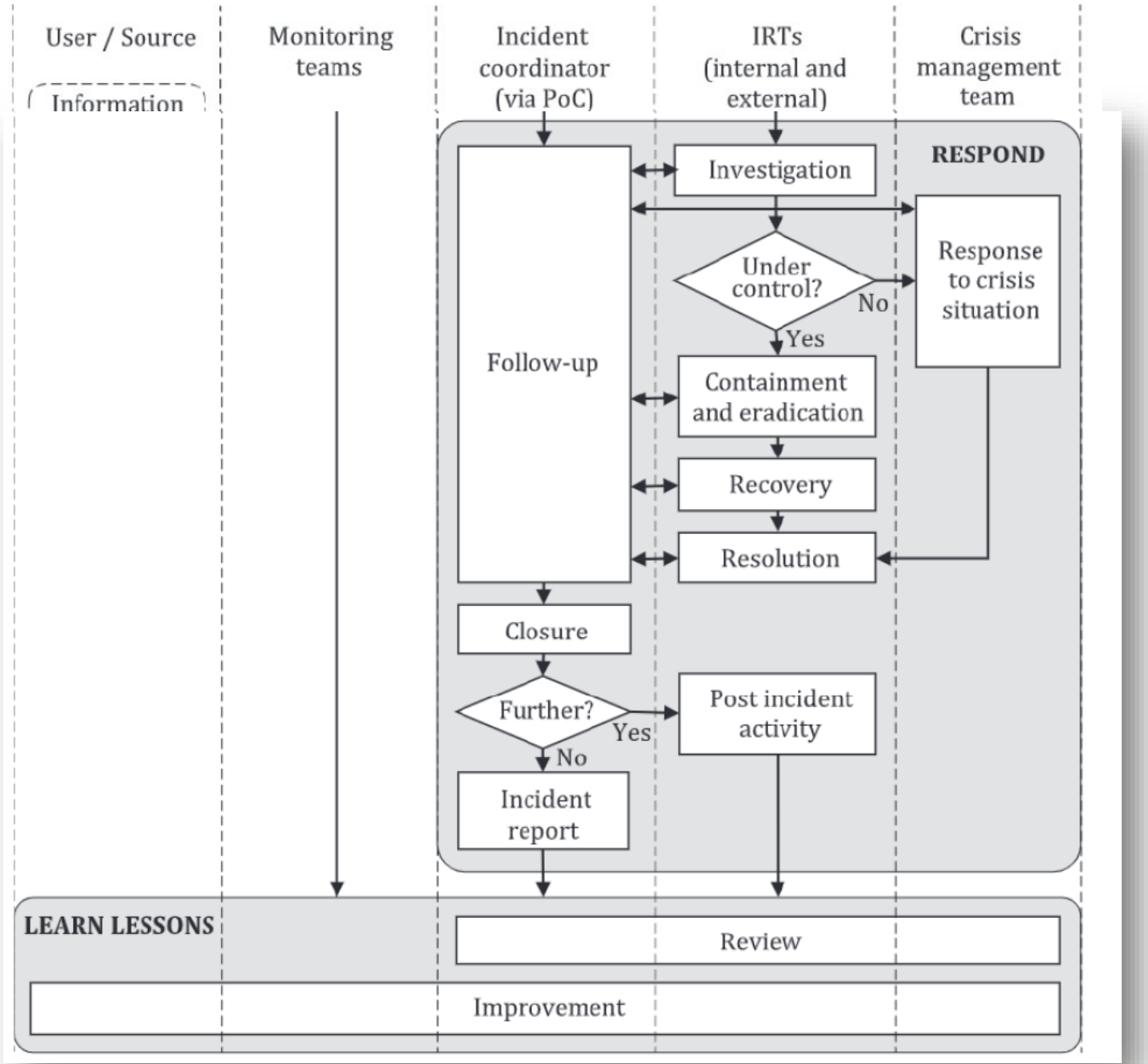
1. Improving overall information security
2. Reducing adverse business consequences
3. Strengthening the focus on information security incident prevention
4. Improving prioritization
5. Supporting evidence collection and investigation
6. Contributing to budget and resource justifications
7. Improving updates to information security risk assessment and treatment results
8. Providing enhanced information security awareness and training programme material
9. Providing input to the information security policy and related documentation reviews

Incident management structure

- **Teams:**
  - IMT, PoC, Incident coordinator
  - Incident response team
  - Crisis management team
  - Vulnerability management team
  - Security monitoring team
  - Awareness and training team
  - Change management team (?)



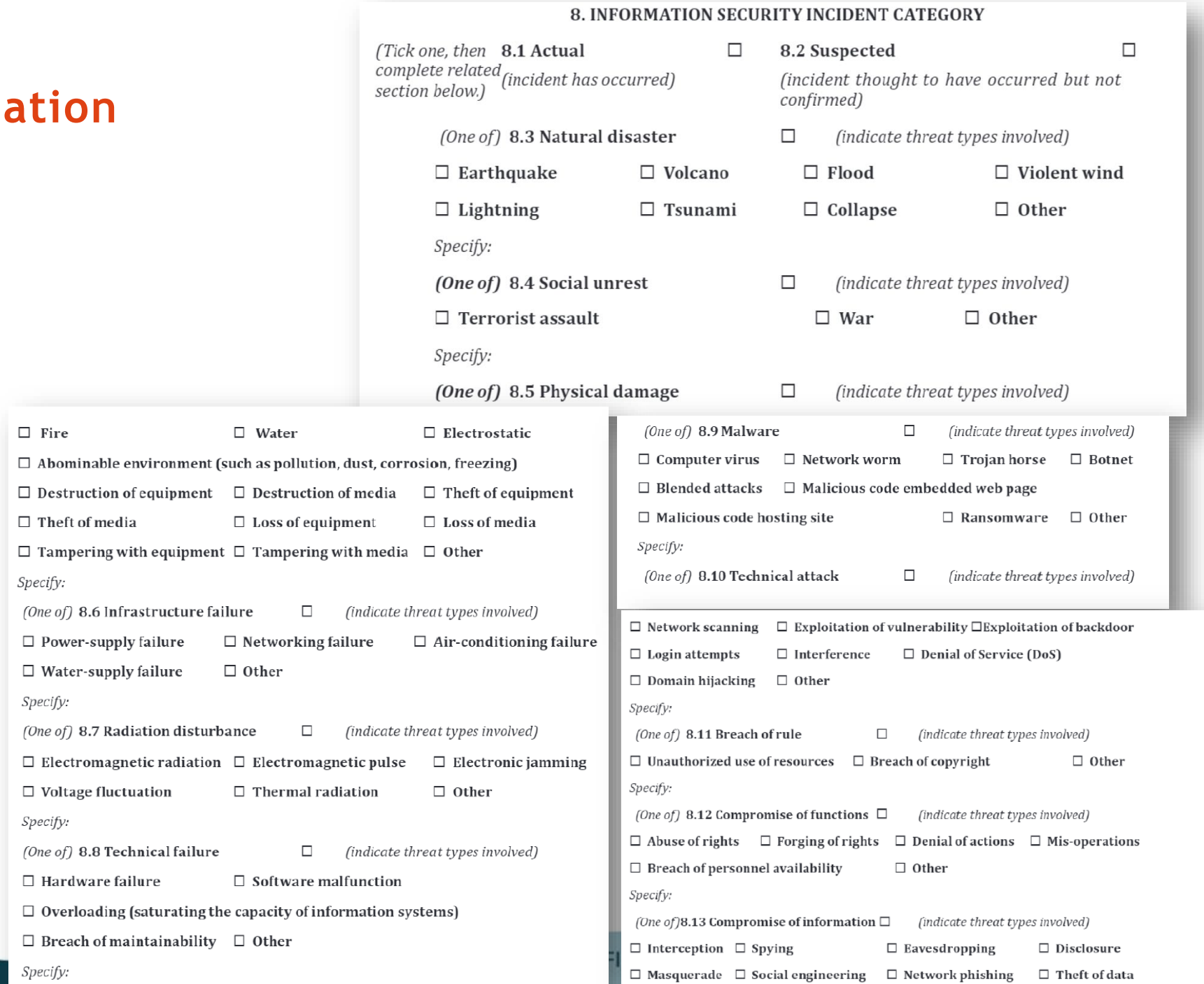

User / Source
Monitoring teams
Incident coordinator (via PoC)
IRTs (internal and external)
Crisis management team
Information security event
PLAN AND PREPARE
DETECT AND REPORT
Detection
Detection
Event report
Event report
ASSESS AND DECIDE
Assessment
Yes
incident?
No
Event report


User / Source
Information
Monitoring teams
Incident coordinator (via PoC)
IRTs (internal and external)
Crisis management team
RESPOND
Investigation
Under control?
No
Yes
Response to crisis situation
Follow-up
Containment and eradication
Recovery
Resolution
Closure
Further?
Yes
No
Post incident activity
Incident report
LEARN LESSONS
Review
Improvement

Incident classification

Suggested:

- Type of incidents
  - General
  - Confidentiality
  - Integrity
  - Availability
  - Access control
  - Vulnerabilities
  - Technical failure
- Attacks
  - DoS
  - Unauthorized Access
  - Malware
  - Abuse
- Information gathering



8. INFORMATION SECURITY INCIDENT CATEGORY

(Tick one, then complete related section below.) 8.1 Actual ☐ (incident has occurred) 8.2 Suspected ☐ (incident thought to have occurred but not confirmed)

(One of) 8.3 Natural disaster ☐ (indicate threat types involved)

☐ Earthquake ☐ Volcano ☐ Flood ☐ Violent wind

☐ Lightning ☐ Tsunami ☐ Collapse ☐ Other

Specify:

(One of) 8.4 Social unrest ☐ (indicate threat types involved)

☐ Terrorist assault ☐ War ☐ Other

Specify:

(One of) 8.5 Physical damage ☐ (indicate threat types involved)

☐ Fire ☐ Water ☐ Electrostatic

☐ Abominable environment (such as pollution, dust, corrosion, freezing)

☐ Destruction of equipment ☐ Destruction of media ☐ Theft of equipment

☐ Theft of media ☐ Loss of equipment ☐ Loss of media

☐ Tampering with equipment ☐ Tampering with media ☐ Other

Specify:

(One of) 8.6 Infrastructure failure ☐ (indicate threat types involved)

☐ Power-supply failure ☐ Networking failure ☐ Air-conditioning failure

☐ Water-supply failure ☐ Other

Specify:

(One of) 8.7 Radiation disturbance ☐ (indicate threat types involved)

☐ Electromagnetic radiation ☐ Electromagnetic pulse ☐ Electronic jamming

☐ Voltage fluctuation ☐ Thermal radiation ☐ Other

Specify:

(One of) 8.8 Technical failure ☐ (indicate threat types involved)

☐ Hardware failure ☐ Software malfunction

☐ Overloading (saturating the capacity of information systems)

☐ Breach of maintainability ☐ Other

Specify:

(One of) 8.9 Malware ☐ (indicate threat types involved)

☐ Computer virus ☐ Network worm ☐ Trojan horse ☐ Botnet

☐ Blended attacks ☐ Malicious code embedded web page

☐ Malicious code hosting site ☐ Ransomware ☐ Other

Specify:

(One of) 8.10 Technical attack ☐ (indicate threat types involved)

☐ Network scanning ☐ Exploitation of vulnerability ☐ Exploitation of backdoor

☐ Login attempts ☐ Interference ☐ Denial of Service (DoS)

☐ Domain hijacking ☐ Other

Specify:

(One of) 8.11 Breach of rule ☐ (indicate threat types involved)

☐ Unauthorized use of resources ☐ Breach of copyright ☐ Other

Specify:

(One of) 8.12 Compromise of functions ☐ (indicate threat types involved)

☐ Abuse of rights ☐ Forging of rights ☐ Denial of actions ☐ Mis-operations

☐ Breach of personnel availability ☐ Other

Specify:

(One of) 8.13 Compromise of information ☐ (indicate threat types involved)

☐ Interception ☐ Spying ☐ Eavesdropping ☐ Disclosure

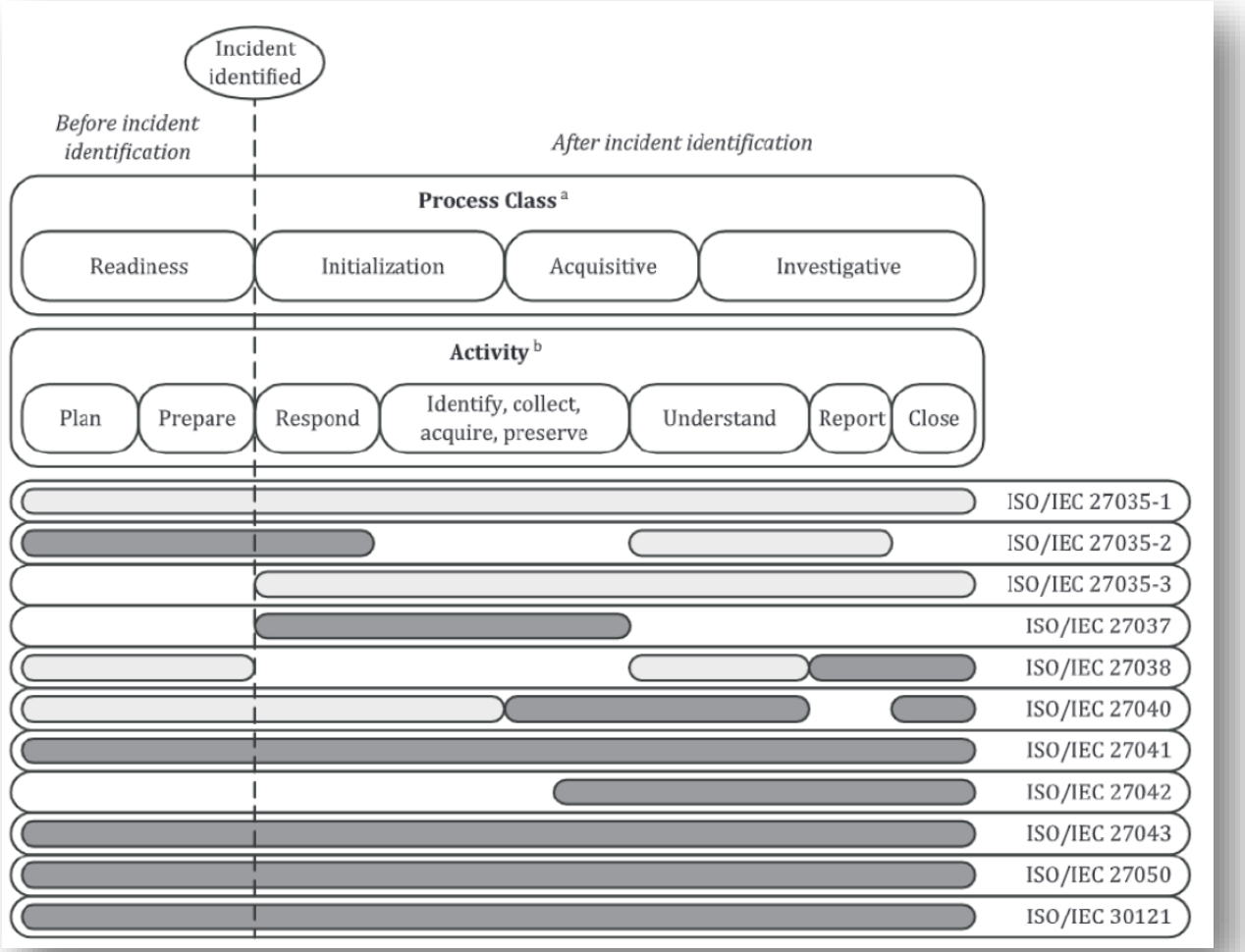
☐ Masquerade ☐ Social engineering ☐ Network phishing ☐ Theft of data

Summary of my opinion on ISO 27035:

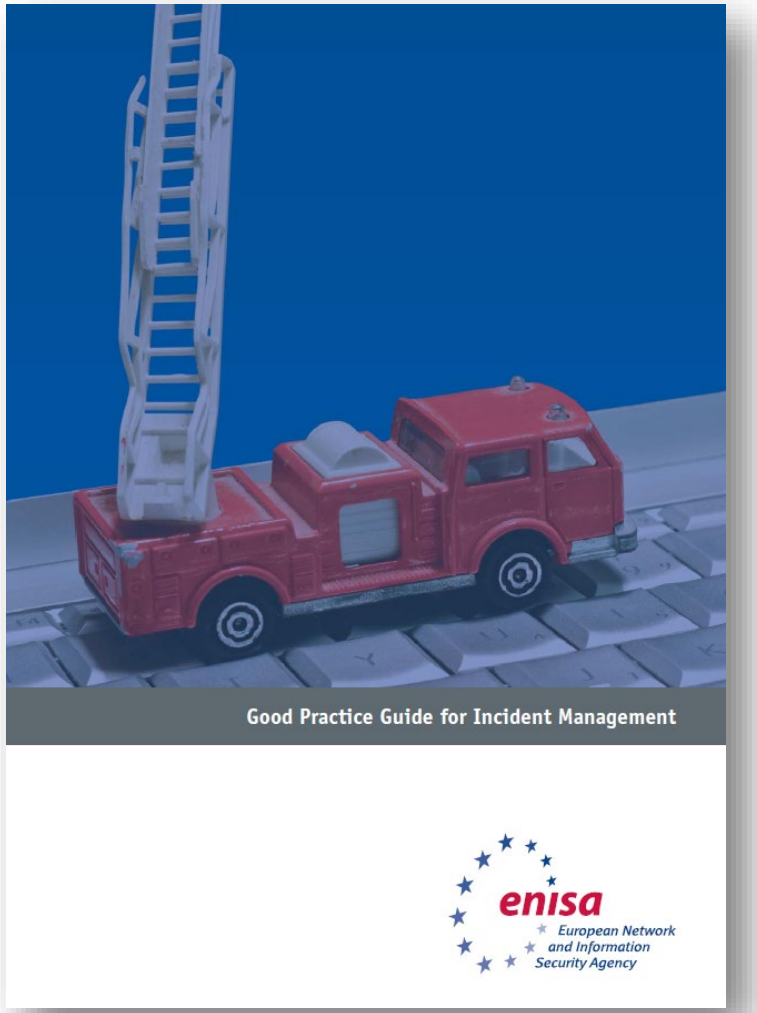
- **ISO 27035 is top-down value for ISO 27001-aligned organizations**
  - ..and most CSIRT/SOCs should implement ISMS for own infosec management
- Standard **provides structure**, but is **a bit short on substance**, i.e. it is not prescriptive
- **Confusion is** introduced by implicit gaps:
  1. Lifecycle of incident (handling)
  2. PoC or ticketing system?
  3. Incident management log vs incident register?
  4. Incident (Analysis? Investigation?) report vs Event report ("6.4 Is the response to this event closed?")
  5. Not clear how vulnerabilities (and threats) are reported (not as Event Report)
  6. Detection: as soon as possible, Reporting: without unnecessary delay, Response: as soon as possible
  7. Detect and alert on anomalous, suspicious, or malicious activities (why not call "infosec events"?)
- **Could lead to fall from the cliff for juniors** (too many "should" to be practical):
  - The event report **should contain** [..] **all circumstances** and facts for comprehension of the event – to classify as incident.

ISO 27035 related standards

- 27037 Digital evidence capture
- 27038 Digital redaction
- 27040 Data storage security
- 27041 Incident Investigation method
- 27042 Analysis of digital evidence
- 27043 Incident investigation principles and processes
- 27050 Electronic discovery
- 30121 Digital forensics risk



So, which one you choose, when?



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

LST ISO/IEC 27035-1:2023

INTERNATIONAL STANDARD

ISO/IEC 27035-1

Second edition
2023-02

Information technology — Information security incident management —

Part 1:
Principles and process

Technologies de l'information — Gestion des incidents de sécurité de l'information —

Partie 1: Principes et processus

ISO IEC

Reference number
ISO/IEC 27035-1:2023(E)

© ISO/IEC 2023