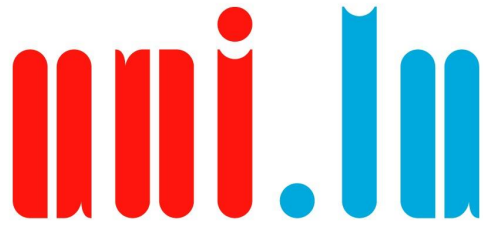


UNIVERSITÉ DU
LUXEMBOURG



UNIVERSITÉ DU
LUXEMBOURG

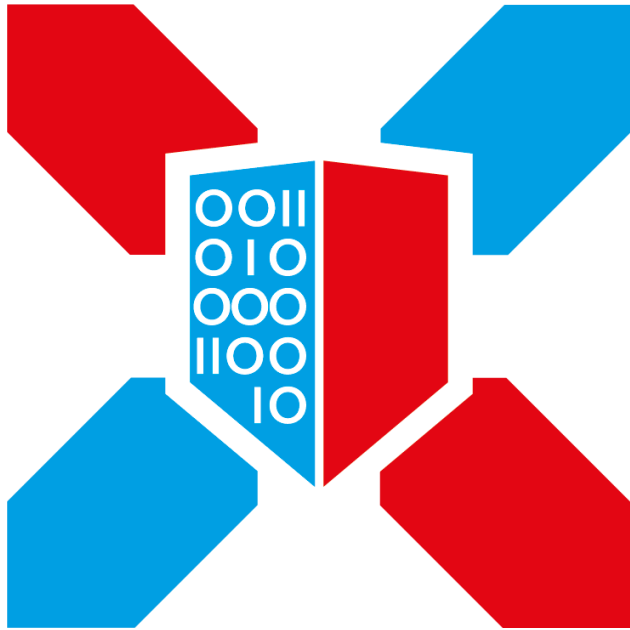
Incident Management

in the context of an
Information Security Policy

Master in Information System Security Management

Part 0

Luxembourg and EU cybresecurity ecosystem



CYBERSECURITY LUXEMBOURG

The Luxembourg Cybersecurity Ecosystem

*20+ years of creating a culture of security
for economic and social prosperity*

WHERE IT ALL STARTED

"I LOVE YOU" VIRUS (2000)



TOWARDS A CULTURE OF SECURITY

OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS (2002)



TODAY

National Strategy IV (2021-2025)

■ Objectives

1. Building trust in the digital world and protection of human rights online
2. Strengthening the security and resilience of digital infrastructures in Luxembourg
3. Development of a reliable, sustainable and secure digital economy

■ Governance Framework

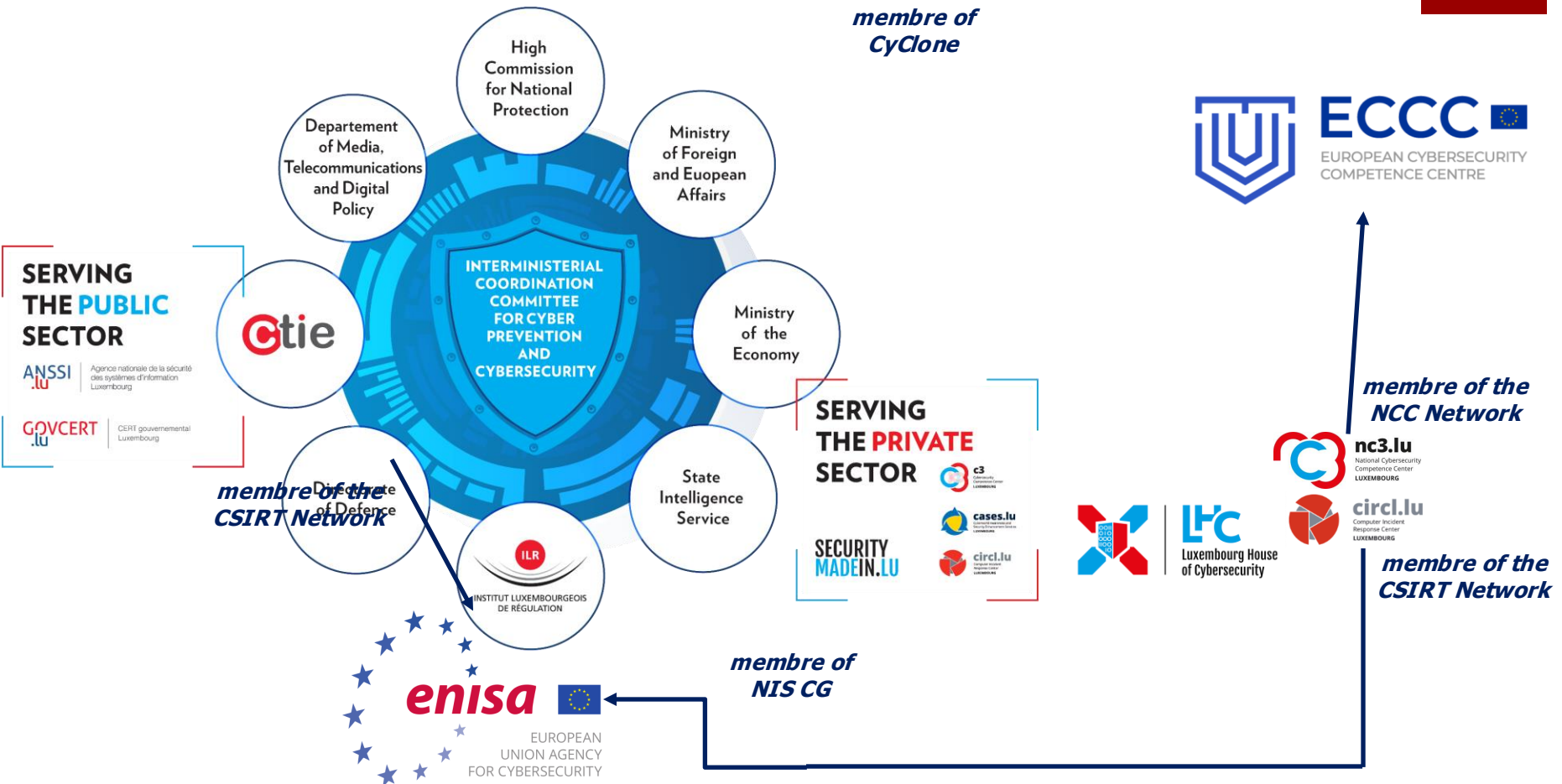
■ Preparedness & Response

■ Education and Awareness

■ Research & Development

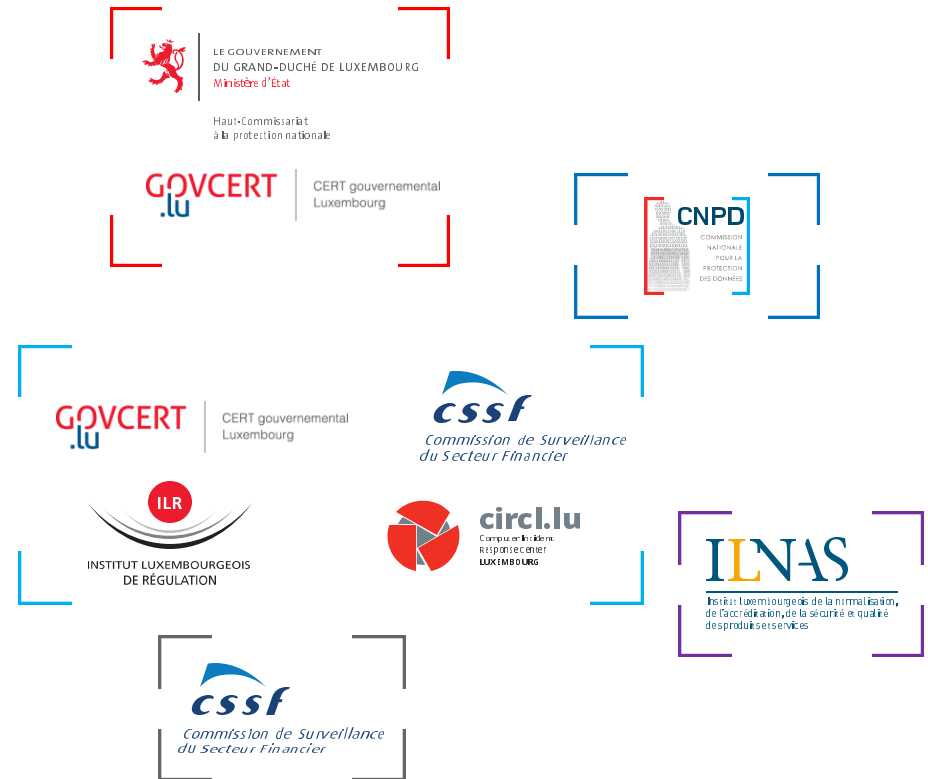


National governance

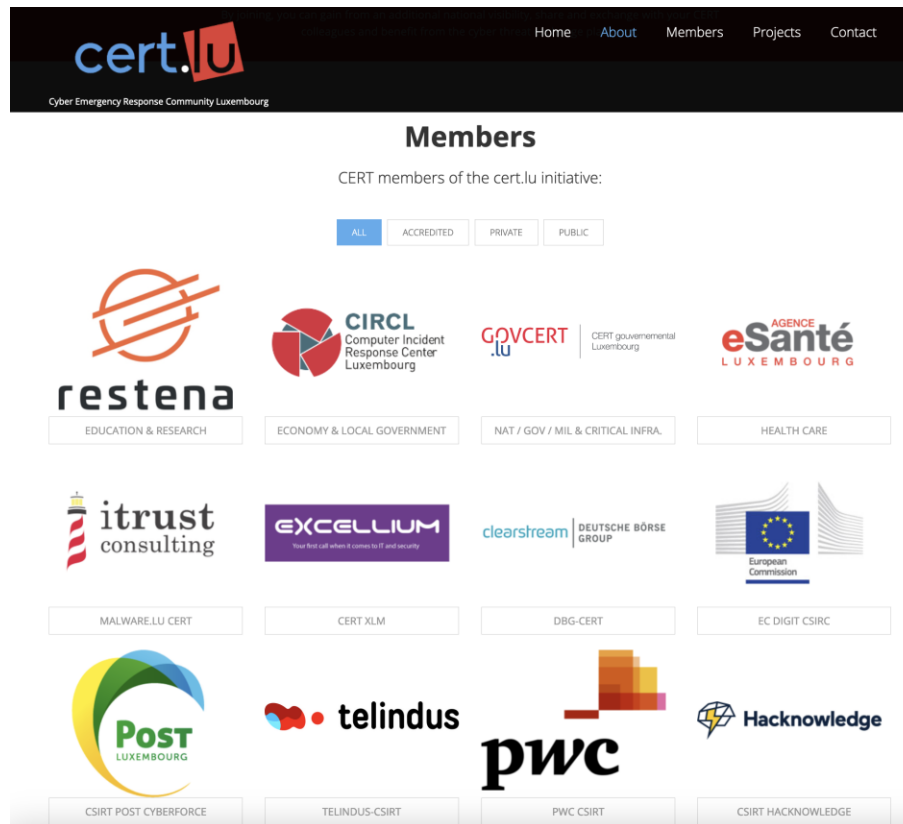


Authorities & Regulators

- **CIP/CER** Critical Infrastructure Protection
(loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale)
- **GDPR** General Data Protection Regulation
(loi du 1er août 2018 portant mise en place du régime général sur la protection des données)
- **NIS(2)** Network and Information Security
(DORA)
(loi du 28 mai 2019 portant transposition de la directive NIS)
- **PSDC** Prestataires de Services de Dématérialisation ou de Conservation
(loi du 25 juillet 2015 relative à l'archivage électronique)
- **PSF** Professionnels du Secteur Financier de Support
(loi modifiée du 5 avril 1993 relative au secteur financier)



Public-private cooperation in Response















cert.lu
Cyber Emergency Response Community Luxembourg

Home About Members Projects Contact

Members

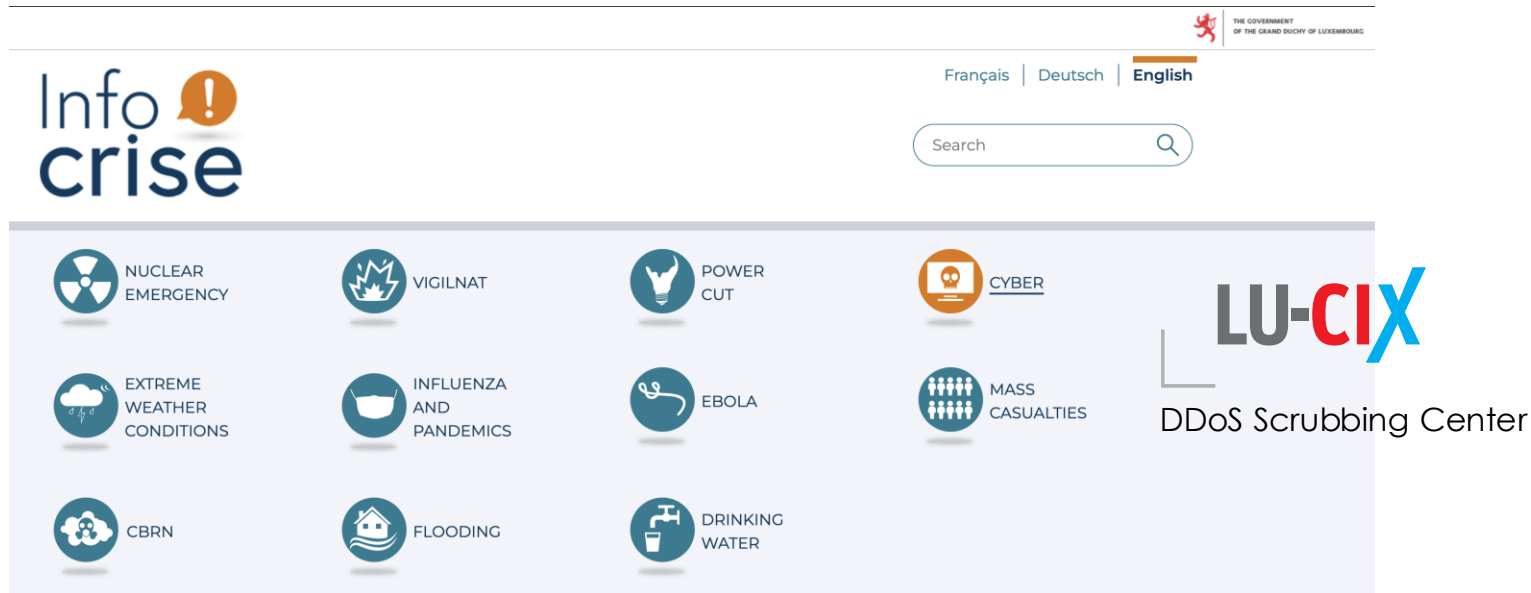
CERT members of the cert.lu initiative:

ALL ACCREDITED PRIVATE PUBLIC

 restena EDUCATION & RESEARCH	 CIRCL Computer Incident Response Center Luxembourg	 GOVCERT.lu CERT gouvernemental Luxembourg	 eSanté AGENCE LUXEMBOURG
 itrust consulting MALWARE.LU CERT	 EXCELLIUM Your first call when it comes to IT and security CERT XLM	 clearstream DEUTSCHE BÖRSE GROUP DBG-CERT	 European Commission EC DIGIT CSIRC
 Post LUXEMBOURG CSIRT POST CYBERFORCE	 telindus TELINDUS-CSIRT	 pwc PWC CSIRT	 Hacknowledge CSIRT HACKNOWLEDGE

LU CERT community

National Preparedness



PIU - Plan d'Intervention d'Urgence

Education and Awareness



- **Master in Information System Security Management**
- **Erasmus Mundus Joint Master in Cybersecurity**
- ***Master in Cybersecurity and Cyber Defence***

- **BTS cybersecurity**



Research & Development



Research & Development



**Competence Hub in
Research in
Cybersecurity and
Cyber Defence**



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign and European Affairs
Directorate of Defence



Faculty of Science,
Technology
and Medicine



Research & Development

Our Funded Chairs

Chair in Capital Markets and Post-Trade



Chair in Cyber Policy



Chair in Digital Procurement



Chair in Entrepreneurship and Innovation



ATOZ Chair in European and International Tax Law



ADA Chair in Financial Law (Inclusive Finance)



Arendt and Elvinger Hoss Prussen Chair in Investment Fund Law



SES Chair in Space, Satellite Communication and Media Law



Chair in Sustainable Finance



UNIVERSITÉ DU
LUXEMBOURG

Public Sector

40

Institutions are part of the ecosystem

[Access the full list →](#)



Access the latest and upcoming International, European and National Legal Frameworks

National contact point



ITY
IRG

SEARCH

DASHBOARD

LOG IN/REGIS

vs & Events

Skills & Jobs

Resources & Support

About

Cont

Private Sector

316

Companies are part of the ecosystem

[Access the full list →](#)



Created during the last 5 years

30

Main point of contact



Number of Startups

74

A closer look to the national actors

National Strategy & Governance



Comité Interministériel en matière de cyber-prévention et de cybersécurité (CIC-CPCS)

[Access the full list →](#)

Preparedness & Response



Research & Development



The Ecosystem Dashboard

Interactive dashboard of the Luxembourg Cybersecurity Ecosystem. It presents a comprehensive overview of the relevant cybersecurity key figures in the Grand-Duchy.



[Ecosystem Overview](#)

Public Sector

Private Sector

A closer look to the private sector

Companies Start-ups

Cybersecurity as core business

Companies have Cybersecurity as their core business

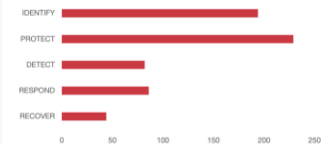
90



ALL COMPANIES COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more →](#)

Diversified solutions offered by the ecosystem



[See more details on the solutions offered →](#)

System view

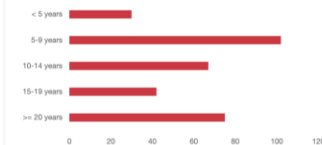
Entities are part of the ecosystem



Public Entities

40

50% of companies have been created in the last 5 years



Join the ecosystem today!

Become an active member of the ecosystem and gain great visibility! Throughout the year, a wide set of actions is organised by the ecosystem for the ecosystem.

[See more information →](#)

Education & Training

Formal Education



[Access the full list →](#)

Initial and Ongoing Training, Re-skilling and Upskilling



[Access the full list →](#)

Awareness Raising Activities



[Access the full list →](#)

Protecting the private sector



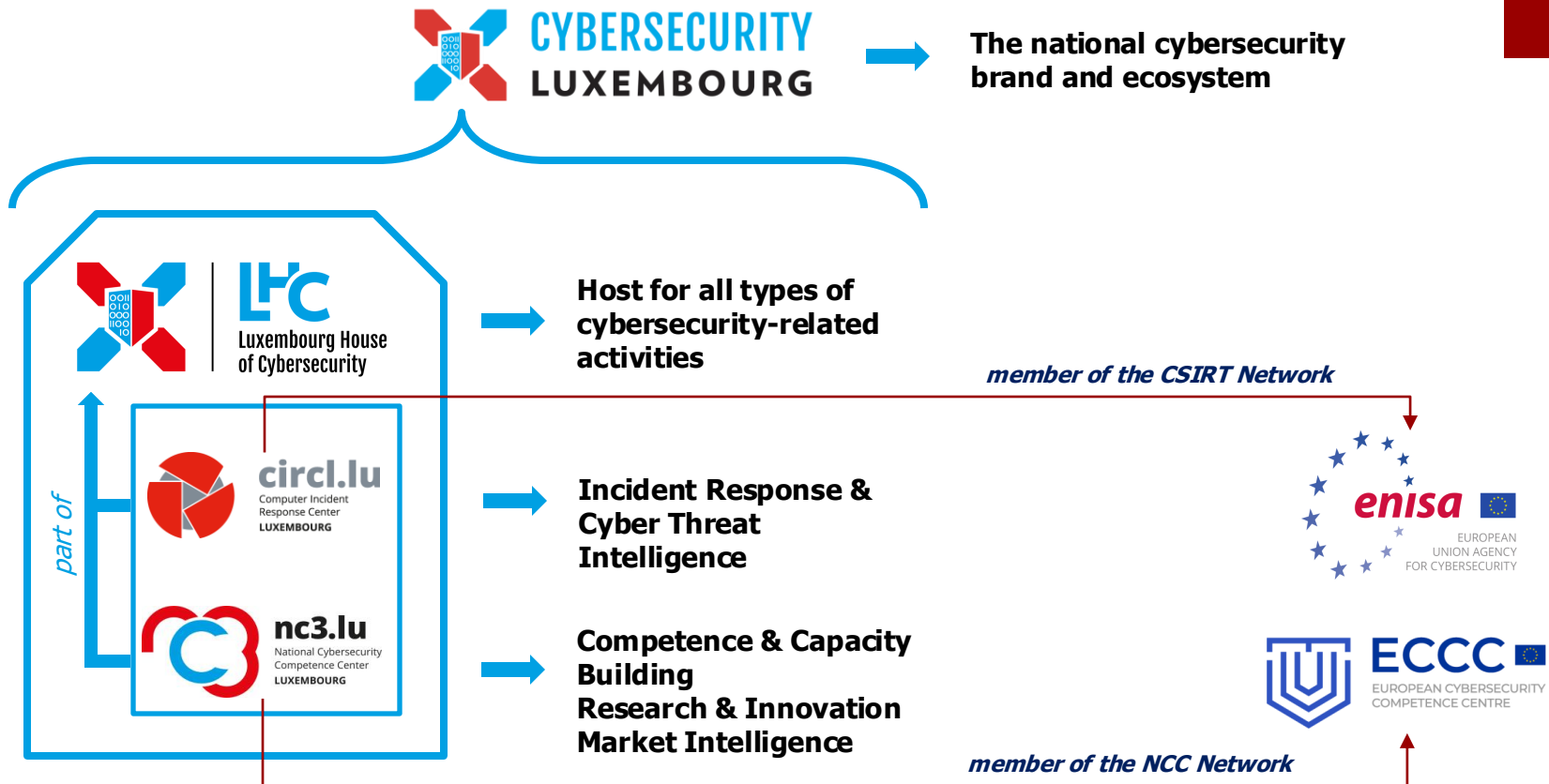
Digital Security Risk Management for Economic and Social Prosperity

OECD Recommendation and Companion Document



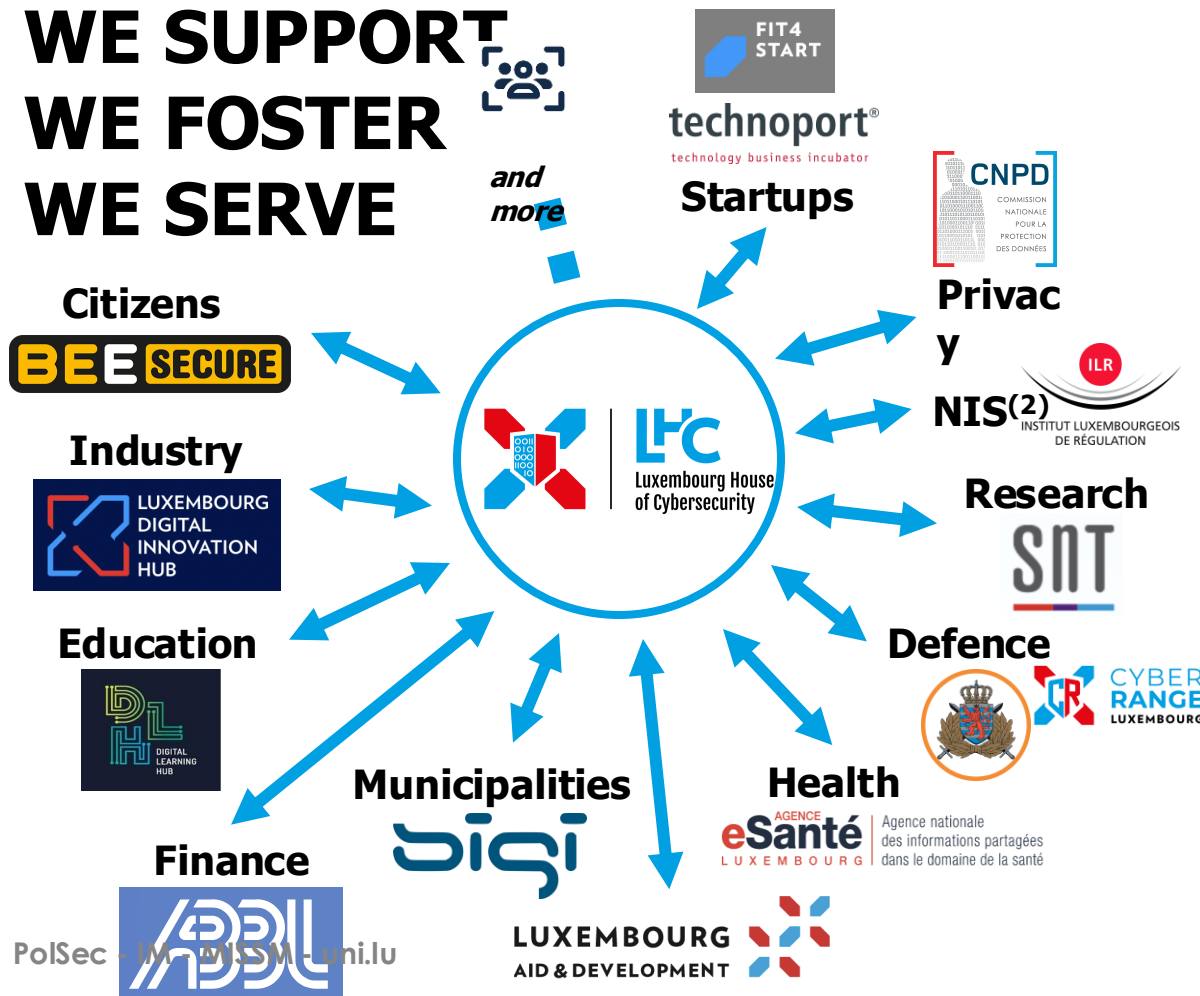
2015

“Digital security risk should be treated like an economic rather than technical issue, and should be part of the organization’s overall risk management and decision-making”



Luxembourg House of Cybersecurity

**WE SUPPORT
WE FOSTER
WE SERVE**



WE HOST



LUCYA

The first **Luxembourg CYbersecurity Accelerator**

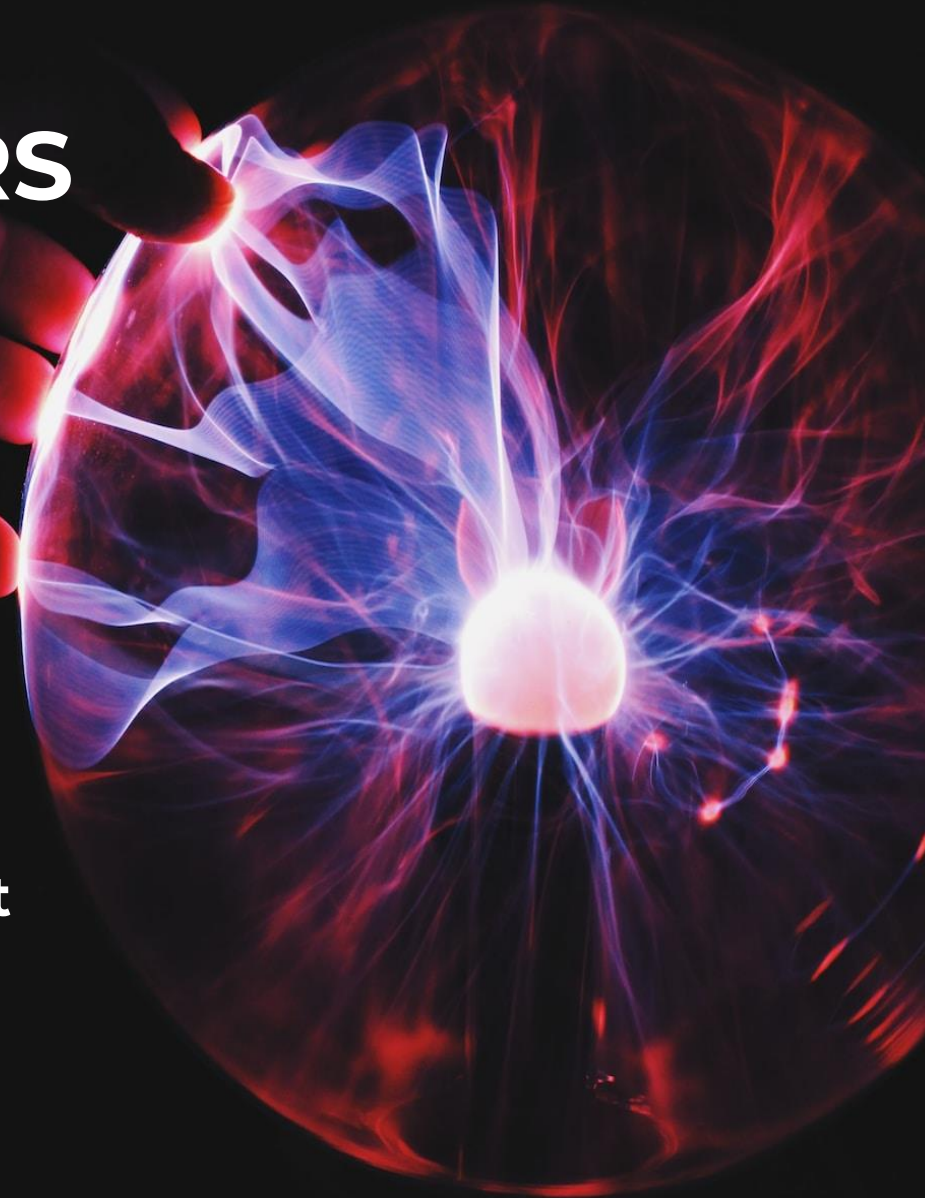
- **Cybersecurity** as a diversification asset contributing to the vitality of the Luxembourg economy

- Operated by  
Luxembourg House
of Cybersecurity

in partnership with **technoport[®]**
technology business incubator

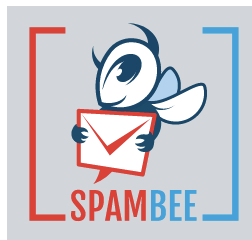
LUCYA'S 4 PILLARS

- 1** Expertise, mentoring & residency
- 2** Access to funding (LU, EU, INT)
- 3** Communication, Events and Community Outreach & international development
- 4**



National Cybersecurity Competence Centre

- Competence and Capabilities Building
- Research, Data and Innovation
- ***NCC-LU***



FIT4CYBERSECURITY - is a self-assessment tool designed for a non-expert audience to estimate in a general way the degree of maturity of its security posture and obtain some basic recommendations.

This tool can be complemented by:

FIT4CONTRACT, to support business owners in verifying if contracts for the procurement of ICT services cover the essential information security aspects.

FIT4PRIVACY, to provide business owners with a good initial overview of their maturity in the field of privacy and data protection (as required by the GDPR).



TOP - aims to support its users with evidence-based information on cybersecurity emerging threats, in order to facilitate their decision-making processes regarding the prevention strategies to be undertaken.



TRUST BOX - is the ideal toolset to raise cybersecurity awareness and empower all users with better cyber hygiene.



TESTING PLATFORM - holds the tools and services that will help organisations to perform basic tests on their most commonly exposed infrastructures, starting with email and web servers.



MONARC - is a tool and a method allowing an optimised, precise and repeatable risk assessment.

LU-CID



Luxembourg Cybersecurity Innovation & Development (*Funding Programme*)

- Promote and **support Innovation** in Cybersecurity contributing to the competitiveness of the Luxembourg economy

- Operated by  **NCC-LU**
LUXEMBOURG CYBERSECURITY
COORDINATION CENTRE

in partnership
with



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie



Co-funded by the
European Union

LU-CID (2)

- **Target** audience:
 - SMEs and start-ups established in Luxembourg
- Projects **topics**:
 - Technical and non-technical cybersecurity **solutions**
 - Affordable cybersecurity assessment or **testing** tools & services
 - Sustainable **open-source** business models
 - Development of cybersecurity **skills** for SME's
- Maximum amount of funding per project: 60'000 €
 - **50% EU / 50% LU**



- *2 rounds of calls opening Q1 & Q4 2024*



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

LU-CID (3)

■ First LU-CID call - **LU-CID-2024-01**

- Opening: 05/2024
- Submissions: 09/2024
- Assessment period: 10/2024 – 11/2024
- Funded projects “runtime”: 11/2024 – 05/2025 (**6 months**)

■ Second LU-CID Call - **LU-CID-2024-02**

- Opening: 11/2024
- Submissions: 01/2025
- Assessment period: 02/2025 – 04/2025
- Funded projects “runtime”: 05/2025 – 10/2025 (**6 months**)

Computer Incident Response Center Luxembourg

- CSIRT (Incident Coordination and Incident Handling)
- Cyber Threat Intel and support tools
- **CSIRT NIS**



CIRCL TYPOSQUATTING
 Typosquatting finder

TYPOSQUATTING FINDER is a free and public service to quickly find typosquatted domains to assess if an adversary uses any existing fake domains. You can enter a domain to discover potentially typo-squatted domains. An advanced option allows you to select the algorithms used.

CIRCL LOOKYLOO

LOOKYLOO is a web interface that captures a webpage and then displays a tree of the domains that call each other. Lookyloo can be used to test unknown or potential malicious links safely.

CIRCL PANDORA

PANDORA is an analysis framework to discover if a file is suspicious and conveniently show the results. You can safely use this free online service to review files or documents received by a third party.

CIRCL URL ABUSE

URL ABUSE is a public CIRCL service to review the security of an URL (Internet link). Users regularly encounter links while browsing the Internet or receiving emails. When there are some doubts regarding an URL (e.g. potential phishing attacks or malicious links), users can submit an URL for review, and a take-down process of the fraudulent content is initiated.

More public services are listed on <https://www.circl.lu/services/>

CIRCL ALSO OFFERS ACCESS TO PRIVATE SERVICES OR CLOSED COMMUNITIES:

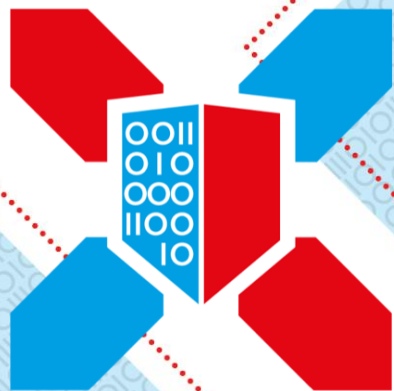
CIRCL MISP
 Threat Sharing

MISP - Open Source Threat Intelligence and Sharing Platform (formerly known as Malware Information Sharing Platform) access is available on request. MISP gives an overview of the current trends of attacks and threat indicators, it is a sharing platform that enables teams to collaborate and provides API access to ingest the information for detection and remediation into the security tools by the organisations.

CIRCL AIL
 Analysis of Information Leaks

AIL LEAK DETECTION AIL Project is an open source framework to collect, crawl, dig and analyse unstructured data, like information leaks publicly available on the Internet or Darknet. Organisations in Luxembourg can benefit from the service by being notified based on contextual keyword lists.

Your gateway to Cyber Resilience



LHC

**Luxembourg House
of Cybersecurity**

Cybersecurity for Europe

- The 3 strategies shaping EU's cyber future
- “Team cyber” for Europe
- Horizon & Digital Europe Programmes
- ECCC, the Network & the Community
a bottom-up approach to achieve cybersecurity excellence for Europe

Strategy for Shaping Europe's Digital Future



European Security Union Strategy



EU Cybersecurity Strategy

1. Resilience, technological sovereignty and leadership
 - NIS2, **ECCC**, cybersecurity shield (SOC), DIHs
2. Building operational capacity to prevent, deter and respond
 - **ENISA**, CERT-EU, JCU, Defense Fund
3. Advancing a global and open cyberspace through increased cooperation
 - Cyber Diplomacy, UN AHC, EUCybernet

“Team cyber” for Europe



- NIS Coordination Group
- CSIRT Network
- CyCLONe (Cyber Crisis Liaison Network)
- The Network (NCCs)
- The Community (Research, Academia, Industry & Civil Society)

ECDC missions

Cybersecurity is a common responsibility and effort, only together can we achieve to cybersecure the EU

- Strengthen EU's **leadership** and strategic **autonomy** on cybersecurity by developing the EU's capacities and capabilities of the Digital Single Market;
- Support and foster **research, innovation** and **technological** developments, for the resilience of systems, including critical infrastructure as well as commonly used hardware and software;
- Encourage and coordinate training activities, to ensure that everyone in Europe has access to the university and **life-long-learning** courses, as well as to motivate young people to go for a **cybersecurity career** and support efforts that address the gender gap; and
- Increase the global **competitiveness** of the EU's cybersecurity industry, ensure high cybersecurity standards throughout the EU and turn cybersecurity into a competitive advantage.

Part 1

Information Security Policy

→ *THE* tool for today's (C)ISO ←

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**.



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.

5	10	15	20	25	
4	8	12	16	20	
3	6	9	12	15	
2	4	6	8	10	
1	2	3	4	5	
FREQUENCY	1	2	3	4	5
	SEVERITY				

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

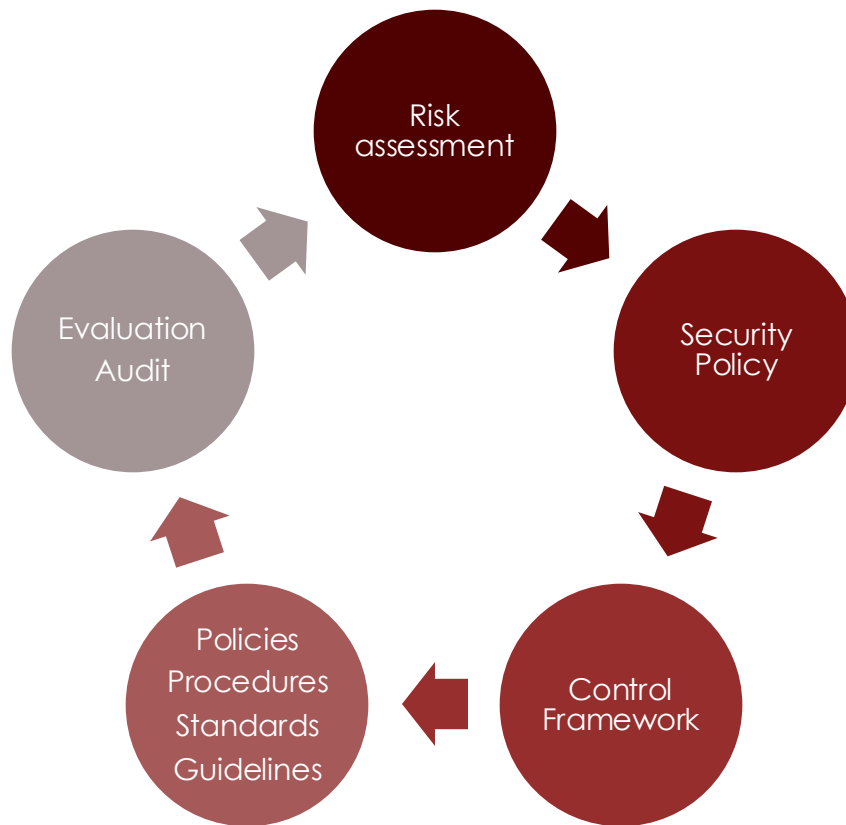
(→ *asset management/classification*)

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1

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 and evaluation

.....

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)*

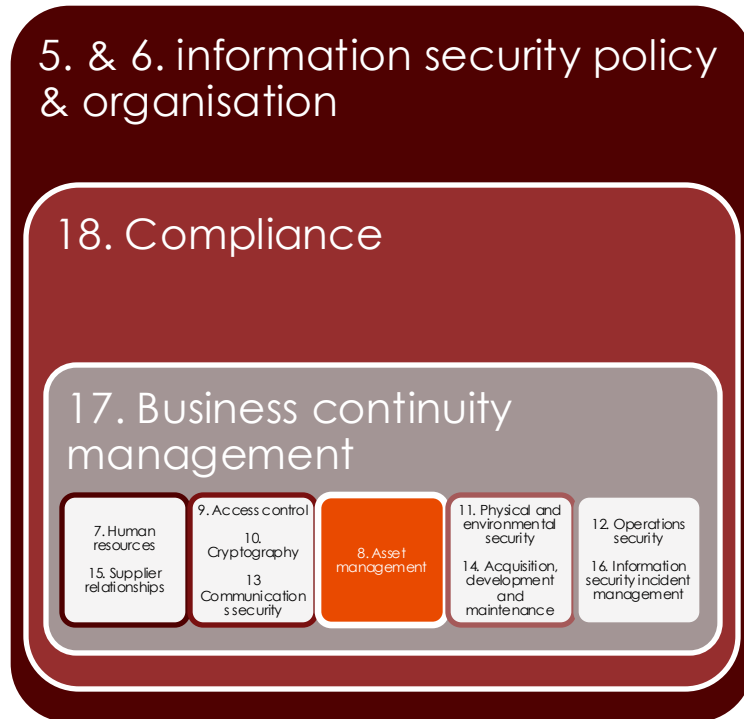
The categorization of controls given in Clauses 5 to 8 are referred to as **themes**:

- 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

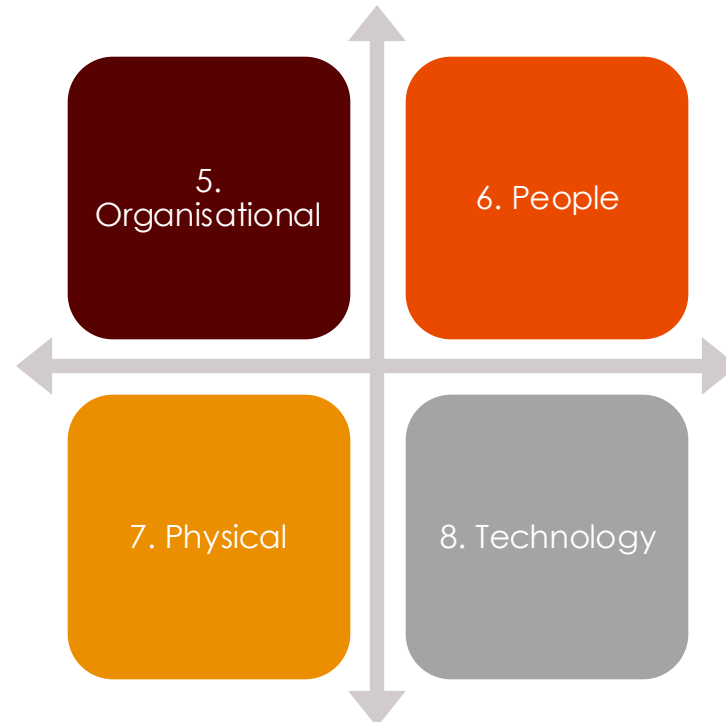
2013

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, references or related documents

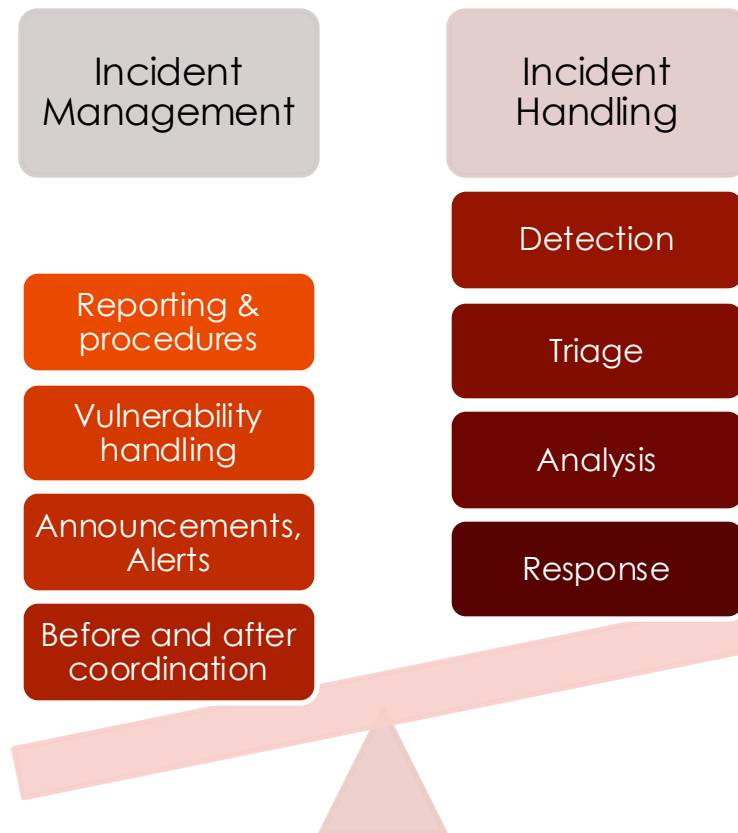
Part 2

Incident **reporting, handling** and **resolution**

Incident Management

in the context of an Information
Security Policy

Management **vs.** Handling



27002 comparison

2013

3 clauses 12 controls

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

2022

4 themes 17 controls

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

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 ISOC

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

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

AMBER

GREEN

WHITE

- **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.

CIA-based classification model

■ Confidentiality

- Secret
- Confidential
- Restricted
- Internal
- Public

■ Integrity

- Vital
- Important
- Normal

■ Availability

- 7
- 6
- 5
- 4
- 3
- 2
- 1

SE	VIT	7
CO		6
RE	IMP	5
IN		4
PU	NOR	3
		2
		1

Reporting

Following: ENISA – Incident Management Guide



Roles & Governance

Following: ENISA – Incident Management Guide

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

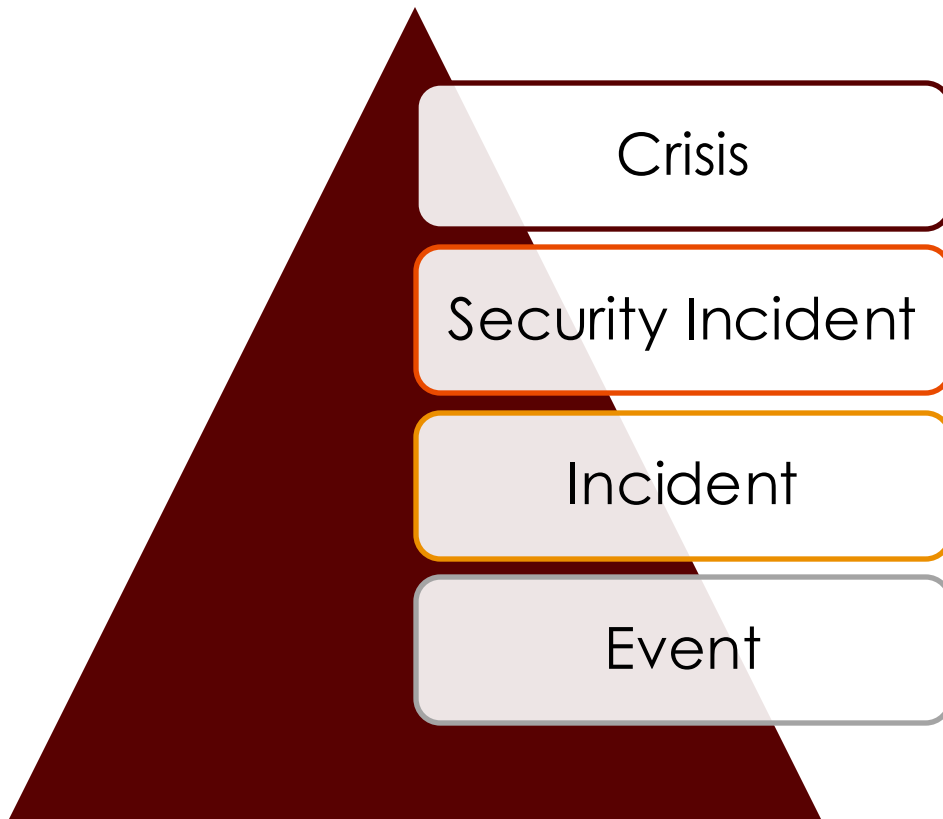
Roles

INCIDENT HANDLER	<p>Analyse incidents assigned to him</p> <p>Resolve incidents²²</p> <p>Fulfil tasks of a duty officer or triage officer if needed</p> <p>Escalate if necessary</p>	<p>Propose improvements in incident handling process</p> <p>Acquire knowledge about new types of incidents</p>	DUTY OFFICER	<p>Ensure that all incidents have owners</p> <p>Be available during service hours</p>	<p>Hand over all remaining work and 'state of the world' to the next duty officer at the end of duty</p>
INCIDENT MANAGER	<p>Coordinate a day within incident handling team; decide how to act in problematic situations</p> <p>Check fulfilment of daily tasks</p> <p>Represent team within the CERT, within the organisation and outside the organisation</p> <p>Advise on how to handle incidents</p> <p>Escalate if necessary</p>	<p>Propose improvements for incident handling team work</p> <p>Discuss balance of incident assignments with incident handlers and triage officers</p> <p>Organise periodic meetings for discussions about incident handling work within team</p> <p>Report to higher management, CISO/CIO, etc</p>	TRIAGE OFFICER	<p>Check for new incidents</p> <p>Filter incidents in terms of their legitimacy, correctness, constituency²¹ (constituency/impact)</p> <p>Hand over incidents to incident handlers in cooperation with the incident manager</p> <p>Report problems with incident</p>	<p>Discuss new kinds of incidents, trends with team members</p>

Handling

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

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:

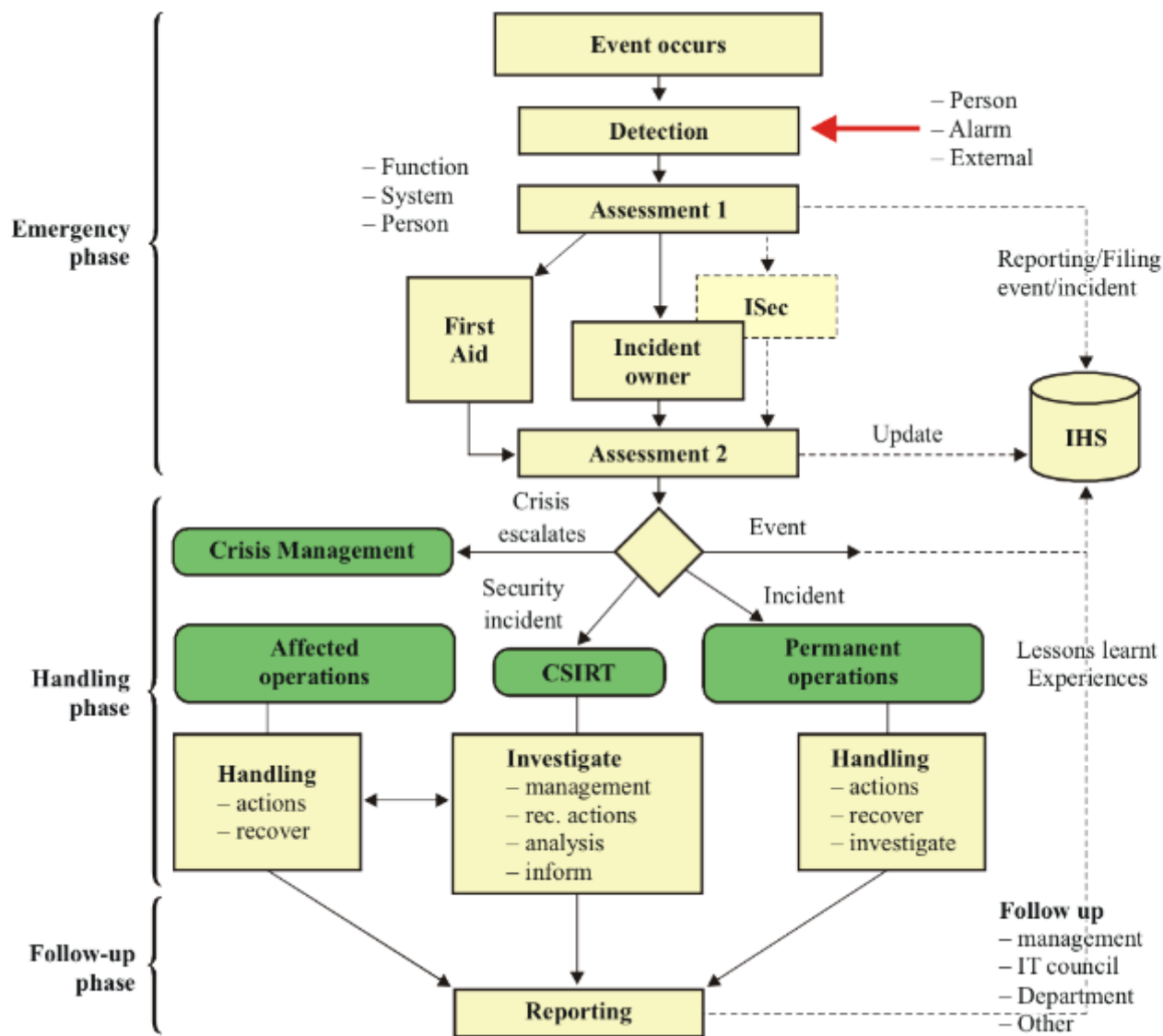
- An event that might have led to an occurrence or an episode which is not serious.

■ 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.*



E.409_F04

Resolution Cycle

Following: ENISA – Incident Management Guide

Incident resolution cycle



(I) Data analysis - collection



- Information to get from the reporter:
 - detailed contact information
 - detailed description of the incident
 - incident classification suggested by the incident reporter
 - logs
 - the exact time of the incident
 - operating systems and network setup
 - security systems setup (eg, antivirus software or firewall)
 - incident severity (in the incident reporter's opinion)

(I) Data analysis - correlation

- Monitoring systems:
 - information related to the IP addresses involved in network monitoring systems (e.g., netflow database).
- Referring database:
 - check if this kind of incident or this incident reporter are already in your incident database.
- Other sources:
 - relevant log-files (routers, firewalls, proxy servers, switches, web application, mail servers, DHCP servers, authentication servers, etc.).



(II) Research resolution

- Based on analysis, team brainstorming on resolution
- Avoid the pitfall of perfectionism
- Sometimes a quick response has the same or a higher value than a comprehensive and complete understanding

ANALYSIS



**RESOLUTION
RESEARCH**

(III) Actions - preparation

- Prepare a set of concrete and practical tasks for each party involved
- Remember to adjust your language

ON
ERY



DATA

RE



**ACTION
PROPOSED**

(III) Actions - internal



RE



- Attack target
 - How to stop and mitigate an ongoing attack:
 - turn off a service
 - check the system for malware
 - patch a system or an application
 - perform or order an audit if you are not able to improve your system security yourself
 - How to deliver more data:
 - concrete practical instructions (e.g. how to obtain a full e-mail header)

(III) Actions - external

■ ISP/ICP

- To collect, save and archive data.
- To monitor network traffic related to the case and inform you if something important happens.
- To filter network traffic in the case of an ongoing attack if such filtering can help to stop or mitigate it.

ON
ERY



DATA

RE



**ACTION
PROPOSED**

(III) Actions - external



- CERTs

- To contact the local ISP/ICP within its constituency
- To ask for advice on how to deal with an incident

- Law enforcement:

- To follow a case if it is significant (e.g. you suspect organised crime activity)
- To assist the reporter of a crime if an incident is to be reported to the police

RE



(IV) Monitor performance

- Basic rules for monitoring the performance of actions:
 - Is the attack target's service turned off?
 - Is the attack target's service still vulnerable?
 - Is the traffic which should be filtered still visible in the network?



(V) Recovery

- Recover or restore to normal the service that was attacked during the incident

**ERADICATION
AND RECOVERY**



**ACTION
PERFORMED**

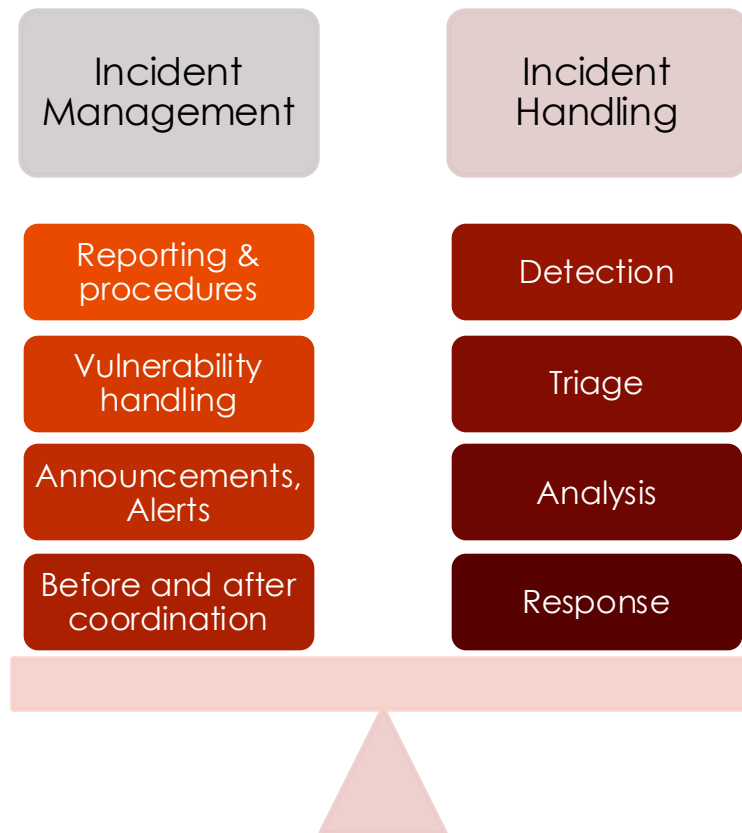


Incident closure, lessons learned & improvements

93

INCIDENT TARGET	ISP/ICP	CERTs	LEGAL	SOURCE OF INCIDENT
COLLECT ALL AVAILABLE LOGS	RETAIN LOGS	MEDIATE CONTACT TO THE LOCAL ISP/ICP	SHARE LEGAL ADVICE	LOG EVENTS
DESCRIBE AN INCIDENT	ASSIST IN OPERATIONAL ACTION	ADVICE IN SIMILAR CASES	SUPPORT LEGAL ACTION	SEARCH FOR SUSPICIOUS USERS
Teach an incident / advise how to avoid it	Explain the mechanism	Share a lesson learnt	Inform about a result / propose a legal action	Advise how to avoid being "an attacker"

Management & Handling

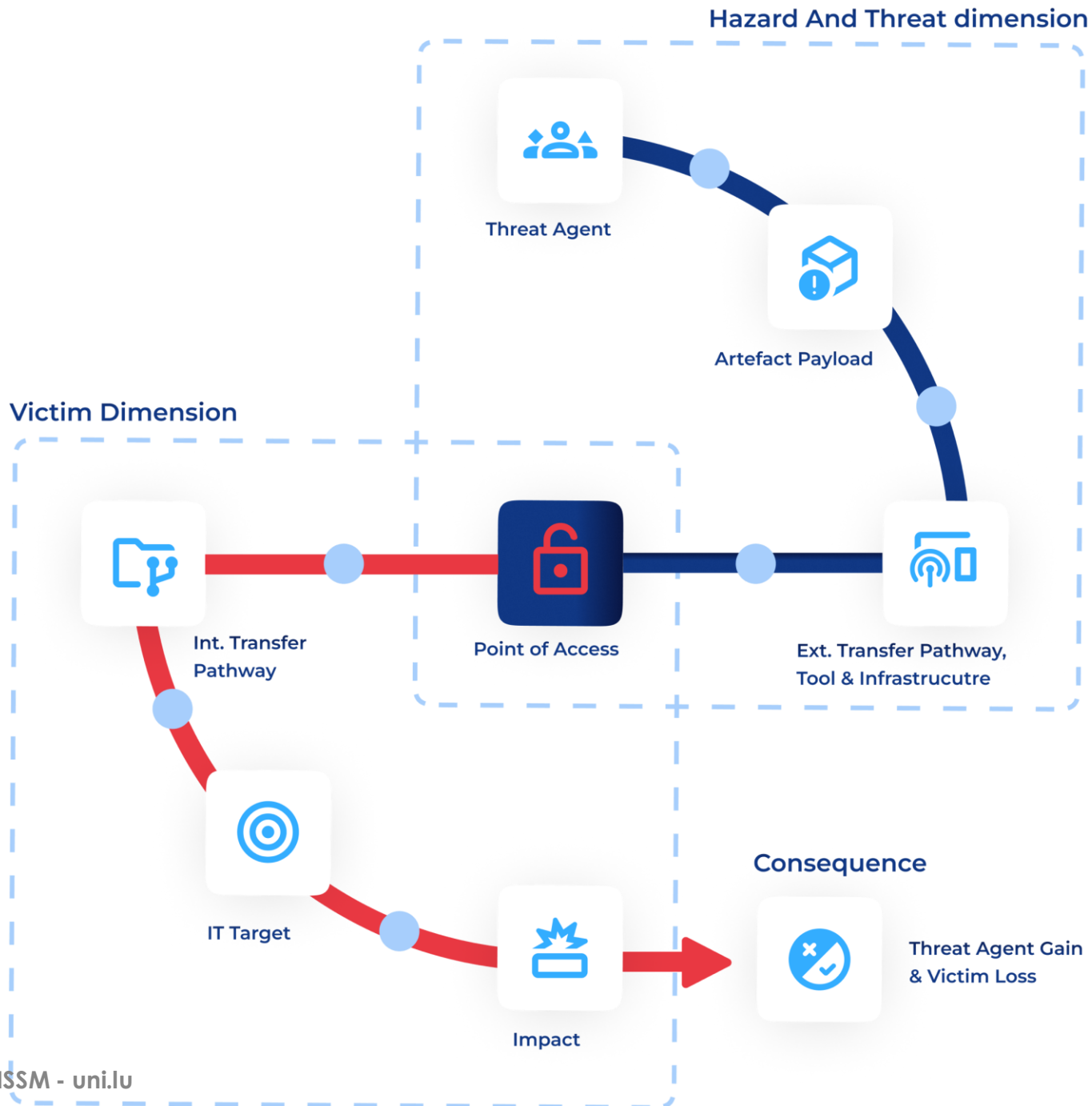


Exam

Homework / Exercice

Threat Observatory

By NC3 – National Cybersecurity Competence
Centre



Q2 2024

General Overview for the the period

Q2 2024

Get a rapid overview of the main cyber security incidents identified and attributed this quarter, along with a trend comparison to the previous quarter.

Threat Landscape

Main Threat Actor ⓘ

APT28 14 ↑ 10

Main External Pathways ⓘ

Phishing 2539 ↑ 335

Main Infrastructures ⓘ

IoT 273 ↓ -73

Main Tools ⓘ

FormBook 142 ↑ 76

[See detail Information & Analysis](#) ↓

Main Access Points & Prevention

Main Access Point ⓘ

CVE 956 ↑ 614

[See detail Information & Analysis](#) ↓

Main Target & Impact

Main Target

Healthcare and public health 16 ↑ 16

Main Impact

Ransom 101 ↑ 64

[See detail Information & Analysis](#) ↓

<https://observatory.nc3.lu/observatory-bulletin/2024/2/>

Exercise

- Choose and understand the threat actor
- Identify and select relevant counter-measures (ISO 27002:2022 controls)
- Define implementation
 - In-house: resources (processes, budget, HR, tools, services, etc.)
 - Out-sourced: partners from the ecosystem
- Describe and argument your choices/decisions
- MAX 3-4 pages

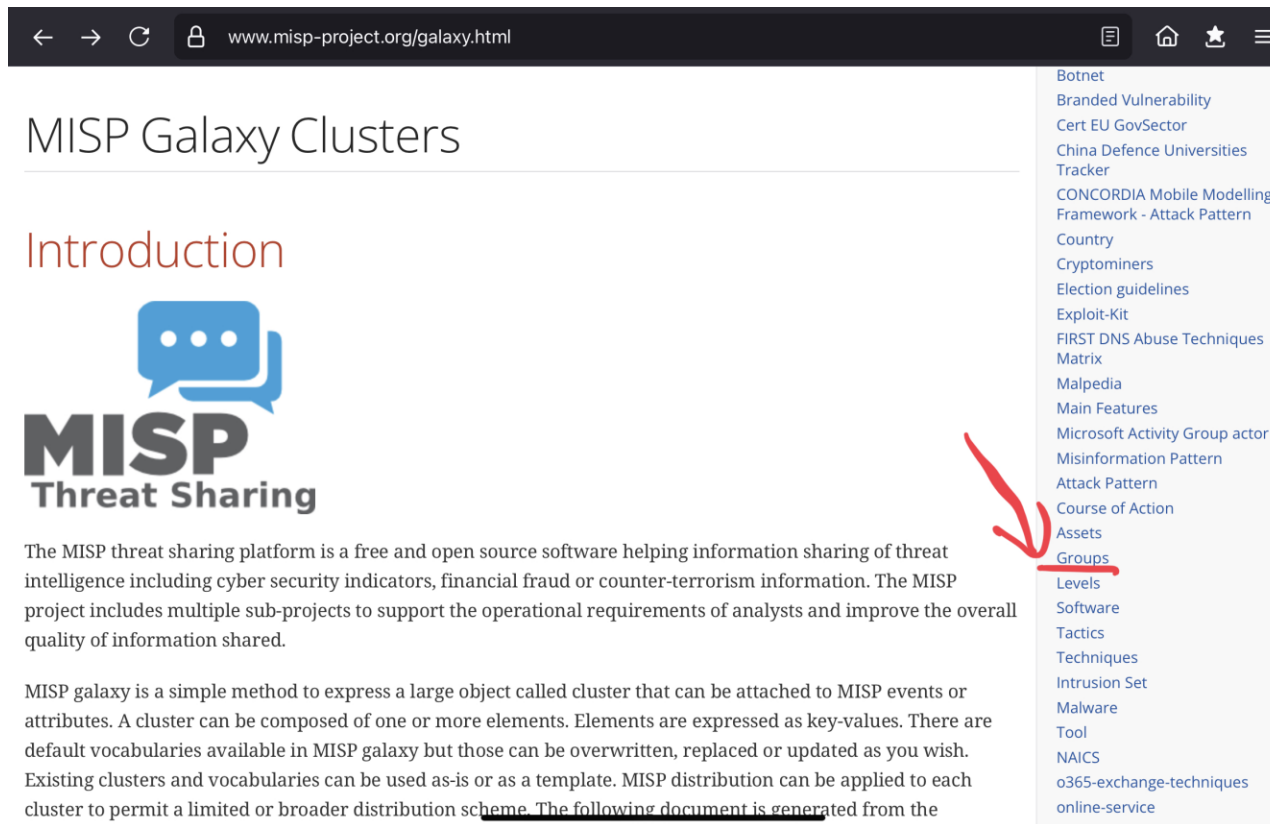


Toolbox

- NC3 Threat Observatory
- MISP *Galaxies*
- ISO 27002:2022
- Cybersecurity Luxembourg Ecosystem
- all other resources you see relevant



MISP (galaxies)



MISP Galaxy Clusters

Introduction

MISP Threat Sharing

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values. There are default vocabularies available in MISP galaxy but those can be overwritten, replaced or updated as you wish. Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme. The following document is generated from the

- Botnet
- Branded Vulnerability
- Cert EU GovSector
- China Defence Universities Tracker
- CONCORDIA Mobile Modelling Framework - Attack Pattern
- Country
- Cryptominers
- Election guidelines
- Exploit-Kit
- FIRST DNS Abuse Techniques
- Matrix
- Malpedia
- Main Features
- Microsoft Activity Group actor
- Misinformation Pattern
- Attack Pattern
- Course of Action
- Assets
- Groups**
- Levels
- Software
- Tactics
- Techniques
- Intrusion Set
- Malware
- Tool
- NAICS
- o365-exchange-techniques
- online-service

<https://www.misp-project.org/galaxy.html>



ISO 27002:2022

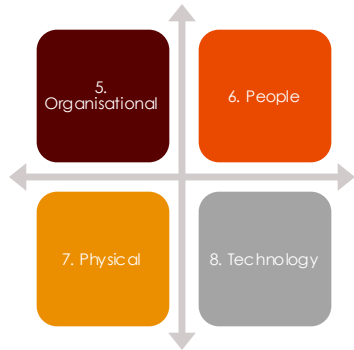
Information security, cybersecurity and privacy
protection – Information security controls

Overview

Themes

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

- a) **people**, if they concern individual persons;
- b) **physical**, if they concern physical objects;
- c) **technological**, if they concern technology;
- d) otherwise they are categorised as **organisational**.



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**

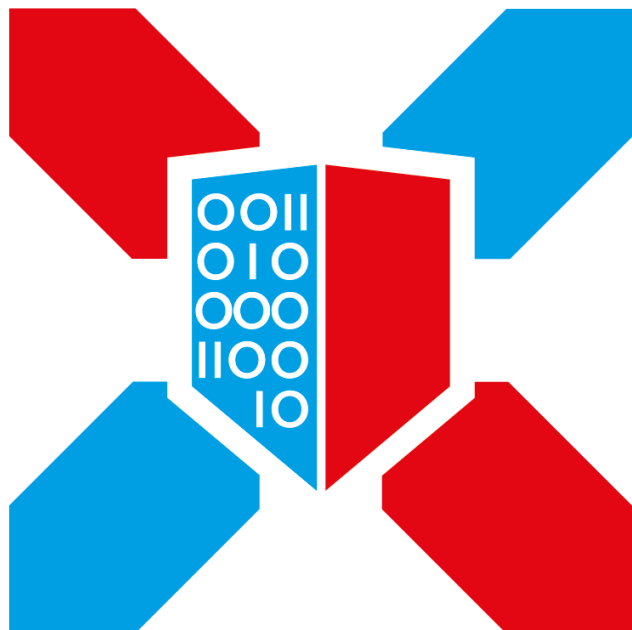
Overview

Attributes (2)

Cybersecurity concepts
attribute values consist of:



- **Identify,**
- **Protect,**
- **Detect,**
- **Respond, and**
- **Recover.**



CYBERSECURITY LUXEMBOURG

The Luxembourg Cybersecurity Ecosystem



SEARCH

DASHBOARD

LOG IN/REGISTER

IMMEDIATE SUPPORT

107

The Ecosystem

News & Events

Skills & Jobs

Resources & Support

About

Contact

The national cybersecurity portal, for everyone

All in one place, explore & be a part of this
community-driven platform whether you are a
seasoned pro or just starting out.

The Ecosystem

How can we help?

<https://cybersecurity.lu>



Latest Alerts



Spear phishing and voice call scams targeting
corporate executives and their accounting...



See all alerts

The Ecosystem Dashboard

Welcome to the interactive dashboard of the Luxembourg Cybersecurity Ecosystem. It presents a complete overview of all relevant cybersecurity key figures in the Grand-Duchy.



Ecosystem Overview Public Sector Private Sector

Private Sector

316

Companies are part of
the ecosystem

[Access the full list →](#)

Main point of contact



Created during the last 5
years

28



Number of Startups

74

Cybersecurity as core business

Companies have
Cybersecurity as their core
business

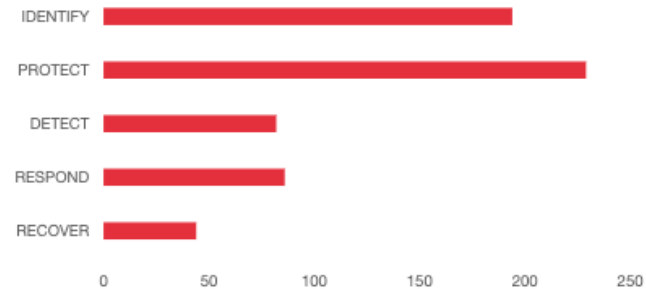
90

316
Companies

● ALL COMPANIES ● COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more →](#)

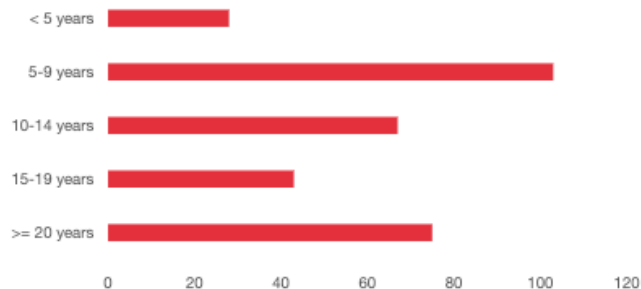
Diversified solutions offered by the ecosystem



● ALL COMPANIES ● COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more details on the solutions offered →](#)

50% of companies have been created in the last 5 years



Join the ecosystem today!

Become an active member of the ecosystem and gain great visibility! Throughout the year, a wide set of actions is organised by the ecosystem for the ecosystem.

[See more information →](#)

Filter by

Clear all

CORE BUSINESS

☐ Cybersecurity

COMPANY TYPE

☐ Start-up

☐ PC Doctors

CLASSIFICATION

1

> ☐ IDENTIFY


> ☐ PROTECT

> ☐ DETECT

> ☐ RESPOND


> ☐ RECOVER

Entities found 316




3C PAYMENT
LUXEMBOURG S.A.

See entity profile →




AbAKUS it-
solutions

See entity profile →




Acarda Services S.à
r.l.

See entity profile →




Accenture Security

See entity profile →



ADNEOM
Luxembourg

See entity profile →



AdronH S.à r.l-S

See entity profile →



Advisory,
Brokerage &
Insurance Leaders



Aedes IT

Thank you for
your attention

CISO community space



<https://lhc.lu/service/luxchat>