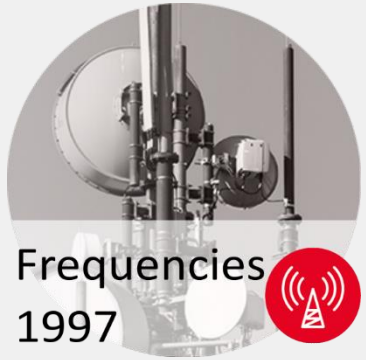
INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

A collaborative approach towards a higher level of cybersecurity

Sheila Becker

17th October 2023


Telecom
1997


Frequencies
1997


Electricity
2000


Postal
2000

ILR


NISS
2019


Airport
2012


Railway
2010


Gaz
2001

Since 2011

- Security Measures in place for Telecom Operators
  - Operators need to provide every year results of their Risk Assessment

Since 2019

ILR – Institut Luxembourgeois de Régulation:

- Competent Authority for :
  - Energy
  - Drinking Water
  - Transport
  - Digital Infrastructure
  - Health
  - DSP

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

ILR'S COLLABORATIVE APPROACH

ILR collaborative, market-oriented approach

Operators share their experiences

Expertise in risk based approach, Neutrality and independance

LIST

common baselines for **cyber risk assessments**.

Objectives in the NIS context

- Apply same principles to OES than for Telecom Operators:
  → Common and sector specific baseline for Risk Assessment
  - Provide operators a tool / platform for :
    - *Security measures;*
    - *Incident notification;*

SERIMA.LU
Security Risk Management

- Means for every sector to:
  → Hold several workshops with the Operators of the different sectors;
  → Define together the common sector specific baseline;

Idea / Objective

- Assuring a common high-level security in all the sectors;
- Achieving a complete view of the sectors on basis of operators individual reports;
- Exchaning information in and with the sectors on risks, vulnerabilities, and threats.

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

SUPERVISION UNDER NIS1

Obligations for operators of essential services (OES)

- Notification of significant incidents
  https://niss-notification.ilr.lu/
  - Per sector: thresholds based on operational impact
  - Impact on availability, confidentiality, integrity of data/networks

Règlement ILR/N22/6 du 03 août 2022

Règlement ILR/N22/6 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur infrastructure numérique

Règlement ILR/N22/5 du 03 août 2022

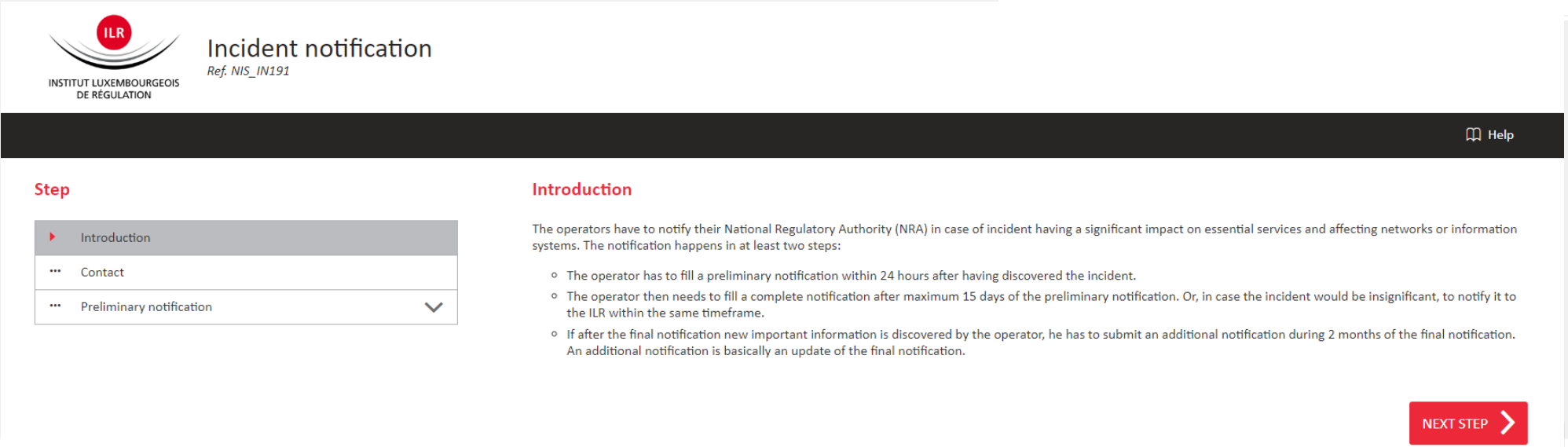
Règlement ILR/N22/5 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur santé

Règlement ILR/N22/2 du 15 juin 2022

Règlement ILR/N22/2 du 15 juin 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport – sous-secteur transport routier

Règlement ILR/N22/1 du 22 février 2022

Règlement ILR/N22/1 du 22 février 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport – sous-secteur transport ferroviaire

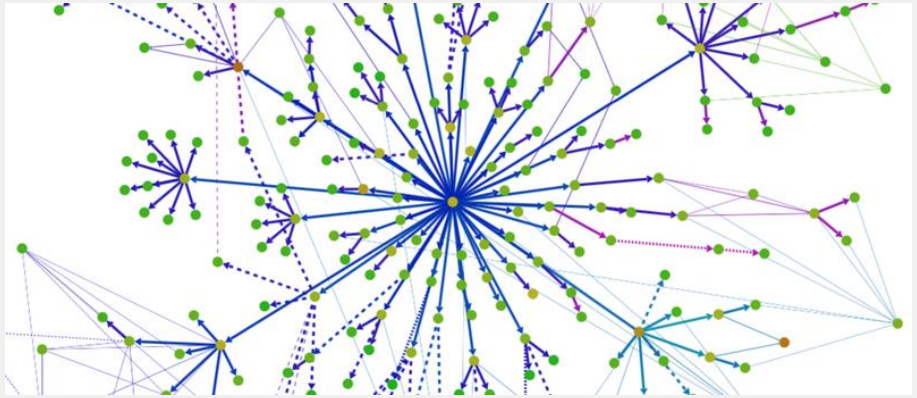


Obligations for operators of essential services (OES)

Règlement ILR/N22/7 du 15 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les opérateurs de services essentiels - NISS.

- Notification of security measures
  - Risk Assessment
  - Security Objectives
  - Dependencies to other essential services

nc3 National Cybersecurity Competence Center LUXEMBOURG MONARC



Security Objective (ENISA)		*Level*
SO1: Information security policy	Establish and maintain an appropriate information security policy	Sophistication level **0** (N/A)
		Sophistication level **1** (basic)
		Sophistication level **2** (industry standard)
		Sophistication level **3** (state of the art)
SO2: Governance and risk management	Establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.	Sophistication level **0** (N/A)
		Sophistication level **1** (basic)
		Sophistication level **2** (industry standard)
		Sophistication level **3** (state of the art)
SO3: Security roles and responsibilities	Establish and maintain an appropriate structure of security roles and responsibilities.	Sophistication level **0** (N/A)
		Sophistication level **1** (basic)
		Sophistication level **2** (industry standard)
		Sophistication level **3** (state of the art)
SO4: Security of third-party dependencies	Establish and maintain a policy, with security requirements for contracts with third parties, to ensure that dependencies on third parties do not negatively affect security of networks and/or services.	Sophistication level **0** (N/A)
		Sophistication level **1** (basic)
		Sophistication level **2** (industry standard)
		Sophistication level **3** (state of the art)

Risks Assessments - Reports we get:

Having as common baseline:

- Set of Primary Assets
- Set of Secondary Assets (scenarios)
- Set of Threats
- Set of Vulnerabilities
- Common risk acceptance level

What the operators provide in their reports:

- Combine the primary assets with the different scenarios
- Assess the impact and the propability of a threat

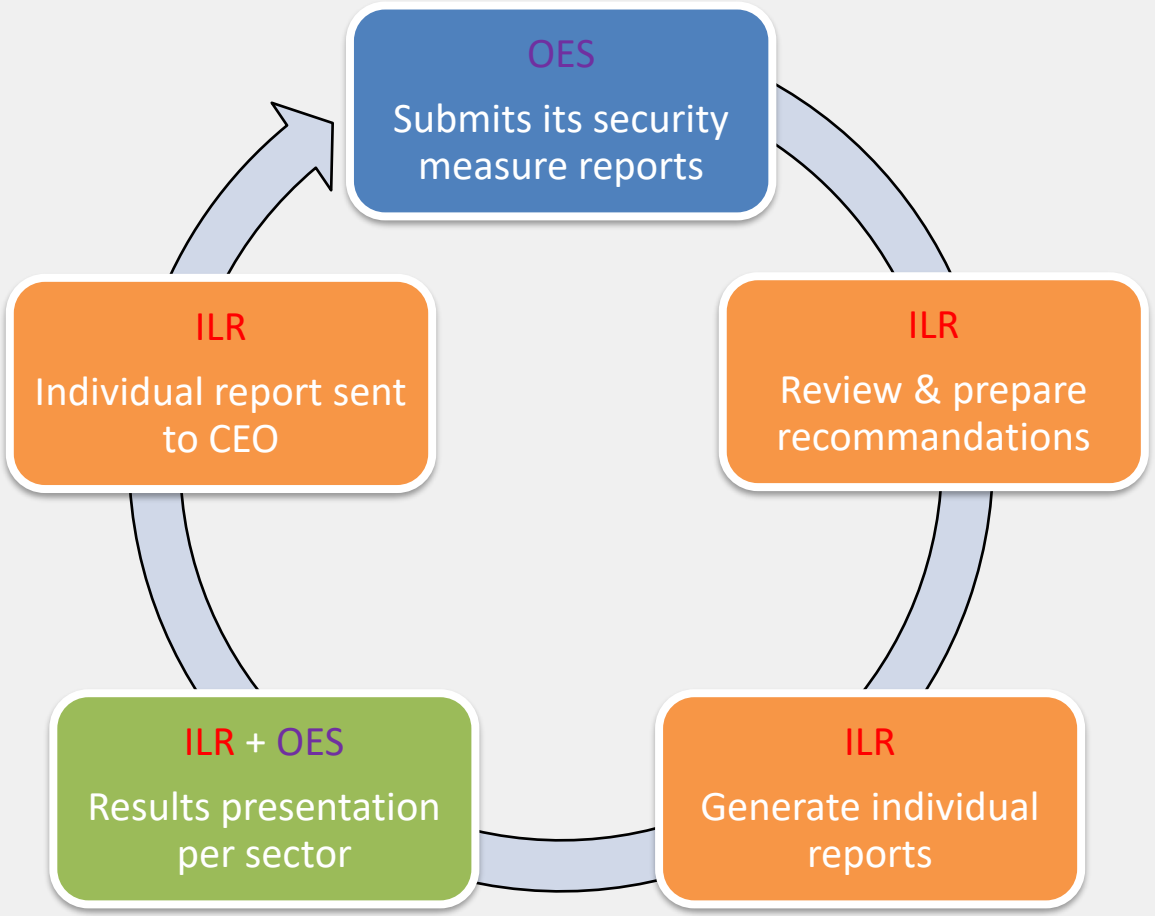
→ Defining the risk level

Risk acceptance level

8

Impact \ Likelihood of occurence	0	1	2	3	4	5
Low	0	1	2	3	4	5
Medium	0	2	4	6	8	10
High	0	3	6	9	12	15
Very high	0	4	8	12	16	20

Current regulatory cycle



INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

INFORMED GOVERNANCE AND ITS BENEFITS FOR SUPERVISION

Does the current approach deliver comparable reports?

→ Not really as entities need to

- Qualify **impacts (CIA).**
- Qualify the **probability of threats.**
- Qualify **ease of exploitation of vulnerabilities.**

Having a common set of primary assets, does not mean that entities take the same scenarios into consideration.

(scenario = threat that exploits a vulnerability of a secondary asset)

There is NO chances, that two distinct entities perform a comparable risk assessment, unless they coordinate and get factual information.

Basics of informed governance

- **Interdependences** between systems are growing and complex, cyber security is **no more an individual challenge**, there is too much at stake.
- Risk management decisions should be **reliable**, **comparable** and **repeatable.**
- **Risk management decisions** should be taken upon as **FACTUAL INFORMATION** as possible.

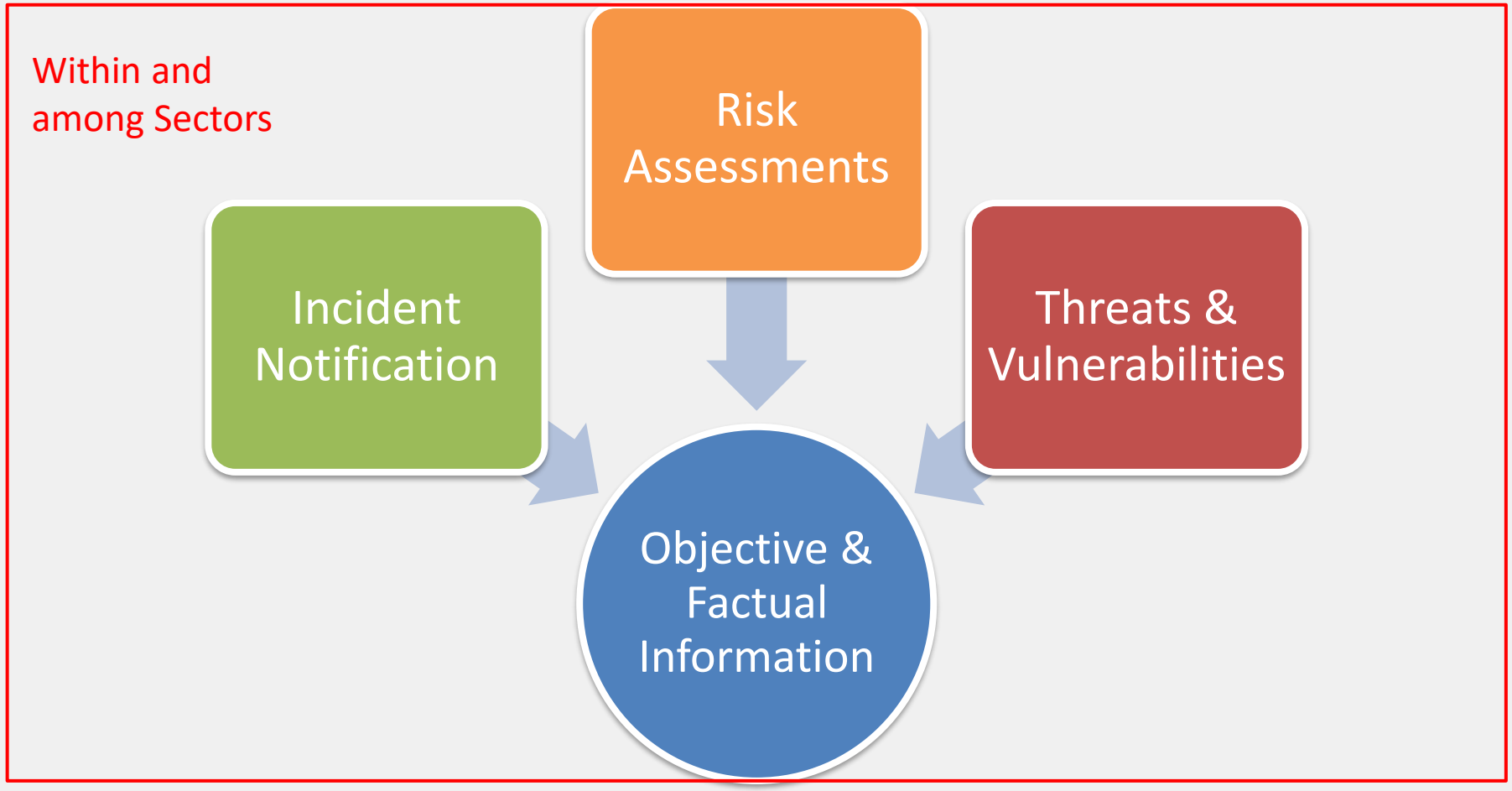
- **Collaboration** is a **MUST, common taxonomies are required**
- **Coordinated guidance** is needed.

- **OCDE document: 2015 -** Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

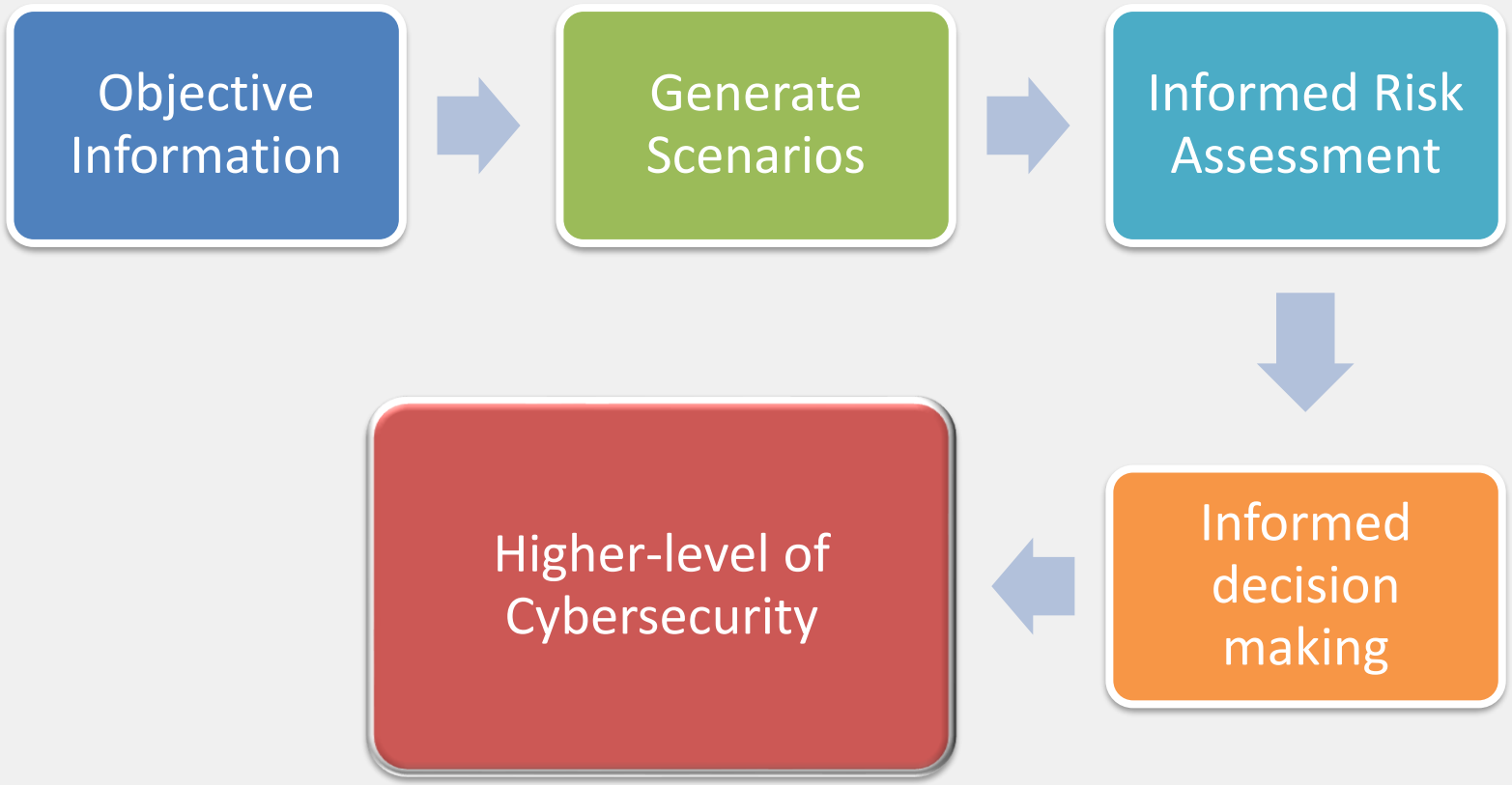
Overall Goal of NIS1 and NIS2

Achieve **high levels of cybersecurity** of network and information systems **across the EU**.

Informed Governance



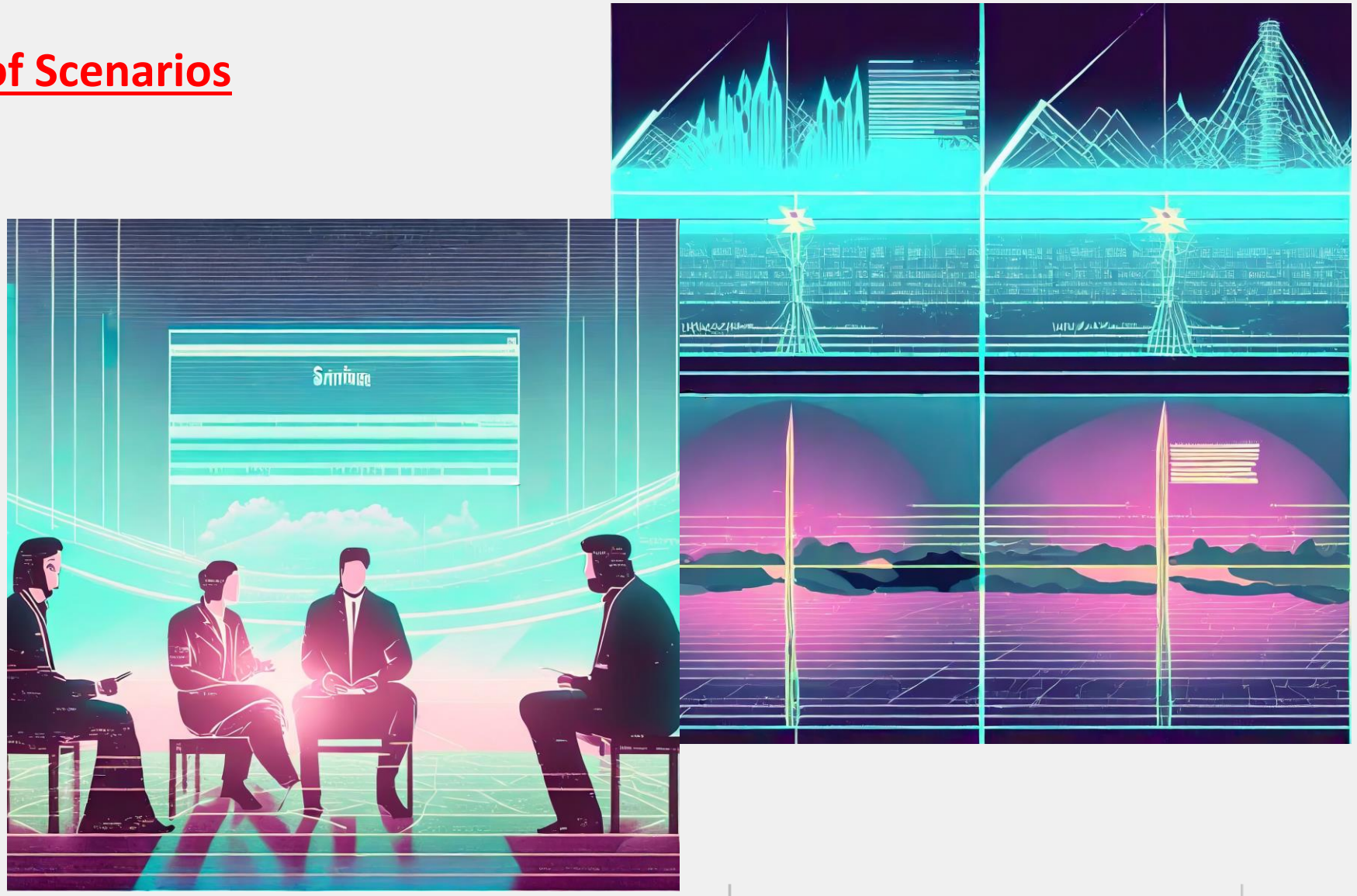
Informed Governance



Why submit to ILR:

- risk analysis, dependencies, security objectives, &
- Incidents ?

Creation of Scenarios



Collaborative approach

- Situational Awareness and incidents must be distilled into scenarios & metrics:
  - Selection of **common scenarios**
  - Qualification of
    - *Threats*
    - *Vulnerabilities*
    - *Effectiveness of treatments*

- Creation of a commonly agreed **taxonomy**
- Raw data must be distilled into **situational awareness (SA)**

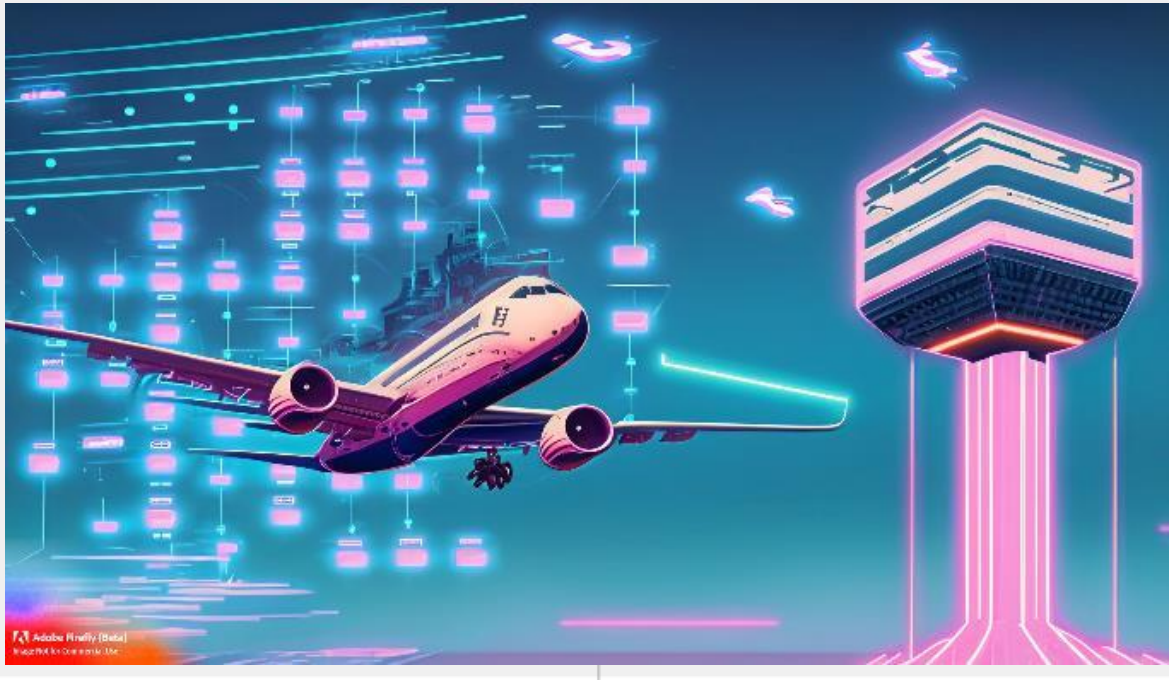
→ Creating guidelines on minimum risk scenarios to be considered by OES together with the sectors.

provide valuable feedback

get factual information

increase the maturity of the sector

reduce systemic risk



INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

SERIMA – A COMMON PLATFORM

Regulatory cycle

- Creating a cyclic process as the environment is constantly evolving;
- Achieving a holistic risk assessment approach;
  - Raising awareness and guidance to operators for:
    - What activities of operators for delivery of the essential service could be at stake;
    - What threats and vulnerabilities could have an impact on those activities;
- Establishing a systematic approach to manage the increasing complexity.

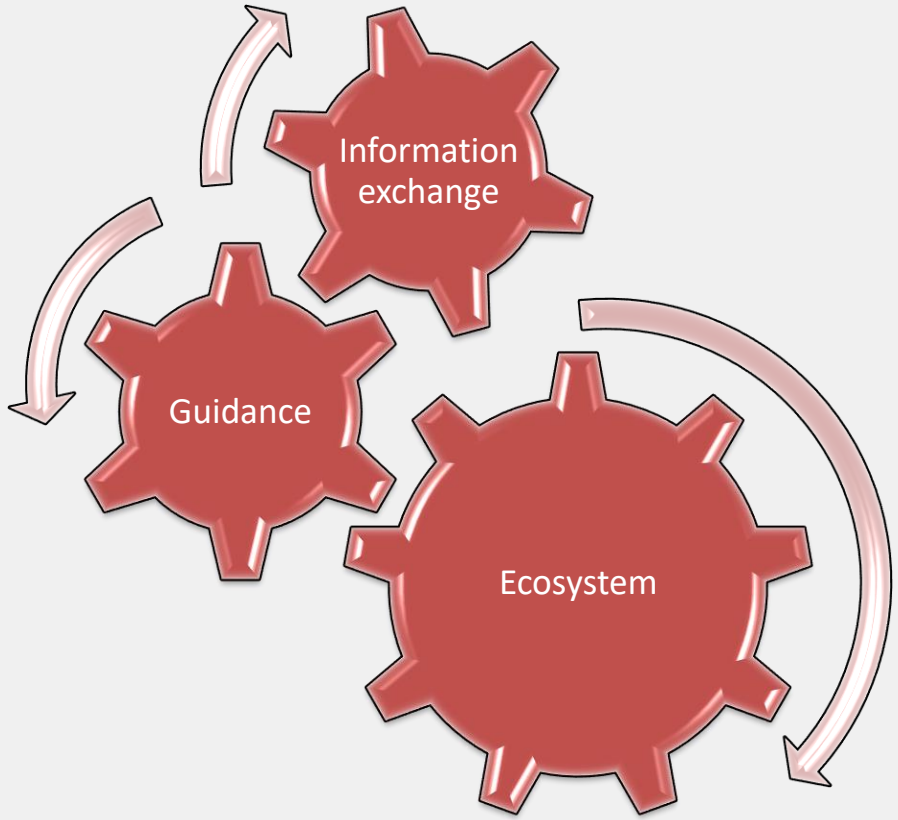
- Modelling the **Luxembourg ecosystem** for the essential entities;
- Perform **risk analysis and systemic risk simulations**;
- Encourage **information exchange**.

Establish the key values:

- Information;
- Awareness;
- Collaboration.

In order to:

- Creating an ecosystem;
- Promoting information exchange within and among sectors;
- Establishing guidance where needed in collaboration with the ecosystem.




LIST


ILR


nc3
National Cybersecurity
Competence Center
LUXEMBOURG
MONARC


LHC
Luxembourg House
of Cybersecurity


SERIMA.LU
Security Risk Management


CENTRE FOR
CYBER SECURITY
BELGIUM


bipt
Belgian Institute for Postal Services
and Telecommunications


SERIMA.be
Security Risk Management
Powered by


circl

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

SUPERVISION UNDER NIS 2

Many companies are unaware that they will be subject to **NIS 2** from **18 October 2024** onwards.

New Sectors

- Telecom
- Trusted Service Providers
- Waste Water
- Managed Service Providers
- Public administration
- Space
- Food Production
- Postal Services
- Manufacturing
- Providers of Social Networks
- Waste Management

What to know about the size-cap?

Definition of SME in NIS2

COMMISSION

COMMISSION RECOMMENDATION
of 6 May 2003
concerning the definition of micro, small and medium-sized enterprises
(notified under document number C(2003) 1422)
(Text with EEA relevance)

(2003/361/EC)

Helpful Guidelines* :

* European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, *User guide to the SME definition*, Publications Office, 2020, https://data.europa.eu/doi/10.2873/255862

Different entity sizes:

- Large entity
- Medium
- Micro & Small

Thresholds *(Article 2)*

Enterprise category	Headcount: annual work unit (AWU)	Annual turnover	or	Annual balance sheet total
Medium-sized	< 250	≤ EUR 50 million	or	≤ EUR 43 million
Small	< 50	≤ EUR 10 million	or	≤ EUR 10 million
Micro	< 10	≤ EUR 2 million	or	≤ EUR 2 million

* European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, *User guide to the SME definition*, Publications Office, 2020, https://data.europa.eu/doi/10.2873/255862

Partnership and linked entities

- Autonomous entity
- Partner entity
- Linked entity

The categories are:

→ **autonomous**: if the enterprise is either completely independent or has one or more minority partnerships (each less than 25 %) with other enterprises (see page 16: 'Am I an autonomous enterprise?');

→ **partner**: if holdings with other enterprises rise to at least 25 % but no more than 50 %, the relationship is deemed to be between partner enterprises (see page 18: 'Am I a partner enterprise?');

→ **linked enterprise**: if holdings with other enterprises exceed the 50 % threshold, these are considered linked enterprises (see page 21: 'Am I a linked enterprise?').

* European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, *User guide to the SME definition*, Publications Office, 2020, https://data.europa.eu/doi/10.2873/255862

Classification Scheme

Introduction of a **size-cap** with the concept of:

- '**essential**' entities ('large-sized') **by default** if:
  - at least **250 employees**
  - or **50 million euros** in sales
- '**important**' entities ('middle-sized') **by default** if:
  - at least **50 employees**
  - or **10 million euros** in sales

Self-registration process!!

Member States may identify 'small-sized entities'

- with a **high risk profile**
- or that are the **sole provider of a service**.

Supervision

- '**essential**' entities
  - ***ex-ante & ex-post** supervision*
- '**important**' entities
  - ***ex-post** supervision*
- On-site **inspections**
- Regular **audits**

- Cybersecurity as a Top Management Priority
- Cyber Hygiene
- Supply Chain Cybersecurity

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

nis2@ilr.lu

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu