



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

## Information session on NIS2

*Sheila Becker*



## Objectif of the session



Demystification of changes coming with NIS2

## Agenda

- **Changes NIS2 is bringing**
- **ILR's approach**
- **Specific changes**
- **Timeline**
- **Collaboration & Support by ILR**



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

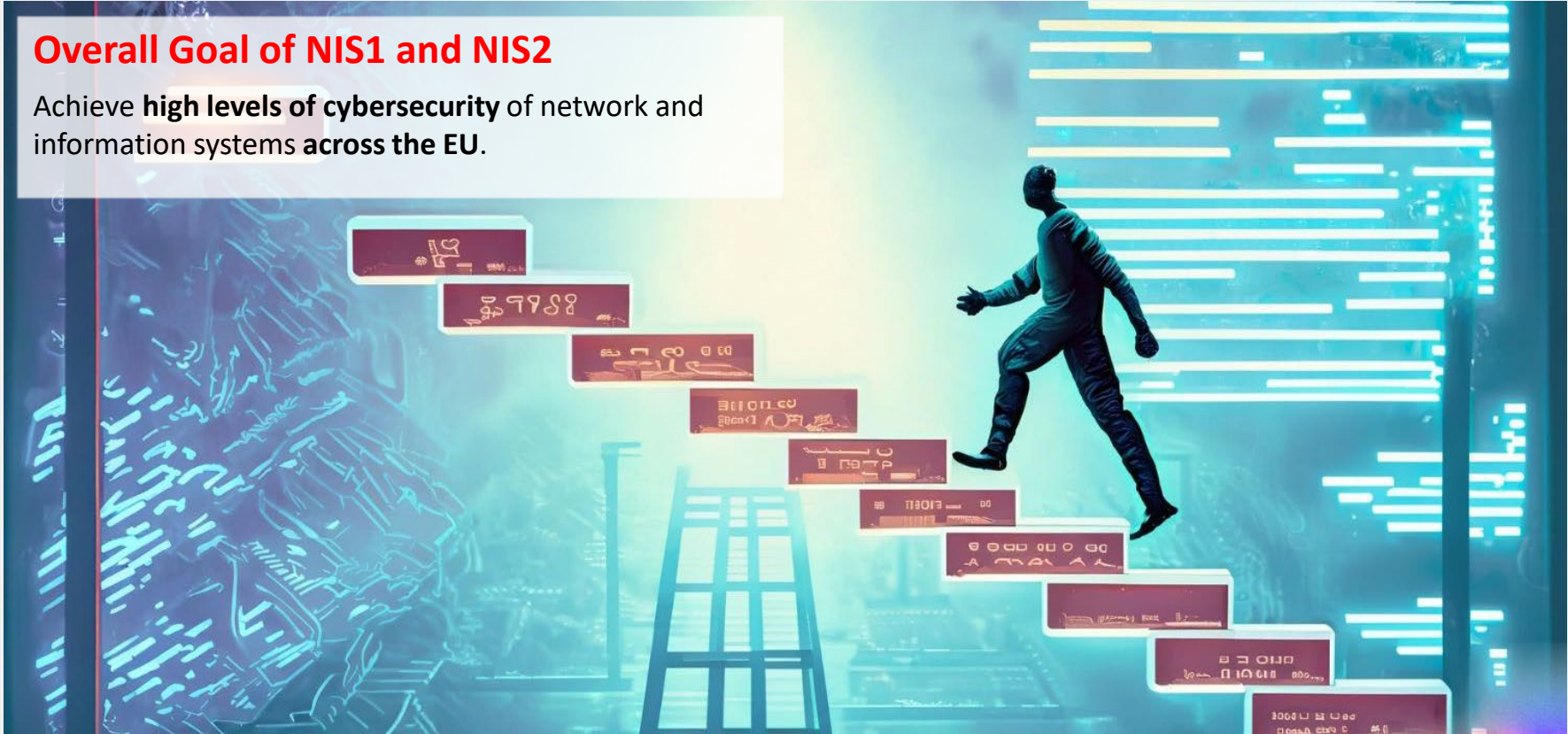
---

# OVERVIEW OF CHANGES NIS2 IS BRINGING



## Overall Goal of NIS1 and NIS2

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





## European Cybersecurity Strategy

### **Cybersecurity Act 2019**

Mandate to establish the EU Agency for  
cybersecurity (ENISA)

Cybersecurity certification framework for  
products and services

### **Cyber Resilience Act 2022 (Proposal)**

Cybersecurity requirements for products with  
digital elements

### **Cyber Solidarity Act 2023 (Proposal)**

European Cybersecurity Shield

Cyber Emergency Mechanism

### **NIS 2 Directive 2022**

Harmonized regulatory approach to  
cybersecurity across the EU

Imposing Cyber Risk Management



- **Scope**
  - **Sectors & size-cap**
  - **Essential & important entities**
- **Governance – C-level**
- **Security measures**
- **Incident Notification procedure**
- **Near-miss notification**
- **Information exchange**
- **Supervision mechanisms by authorities**



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

# OVERVIEW OF CHANGES NIS2 IS BRINGING

→ Scope of NIS2







## 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



Medical Devices

## Classification Scheme

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












- **Large entities :**
  - at least **250 employees**
  - or **50 million euros** turnover
- **Medium entities :**
  - at least **50 employees**
  - or **10 million euros** turnover

→ **By default in Scope**

Member States may identify ‘small-sized entities’

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

## Annex I: Sectors of high criticality

		LARGE	MEDIUM	SMALL
 ENERGY		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 TRANSPORT		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 BANKING		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 FINANCIAL MARKET INFRASTRUCTURE		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 HEALTH		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 WASTE WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
 ICT-SERVICE MANAGEMENT (B2B)		ESSENTIAL	IMPORTANT	NOT IN SCOPE
 PUBLIC ADMINISTRATION		ESSENTIAL	ESSENTIAL	ESSENTIAL
 SPACE		ESSENTIAL	IMPORTANT	NOT IN SCOPE

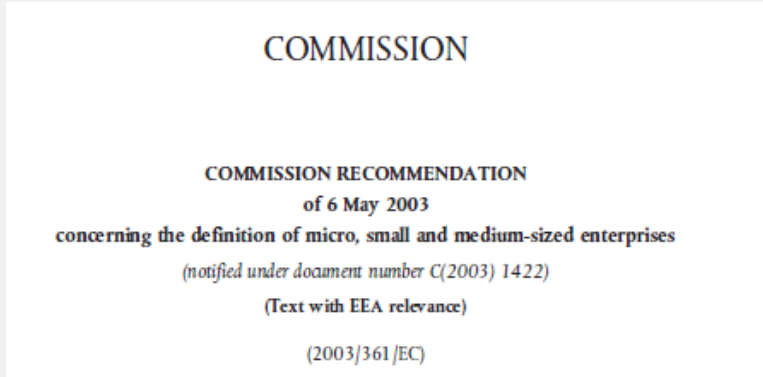


## Annex II: Other critical sectors

		LARGE	MEDIUM	SMALL
<b>POSTAL &amp; COURIER SERVICES</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>WASTE MANAGEMENT</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>PRODUCTION, PROCESSING AND DISTRIBUTION OF FOODS</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>MANUFACTURING</b>	Medical devices and in vitro diagnostic medical devices	IMPORTANT	IMPORTANT	NOT IN SCOPE
	Computer, electronic and optical products	IMPORTANT	IMPORTANT	NOT IN SCOPE
	Electrical equipment	IMPORTANT	IMPORTANT	NOT IN SCOPE
	Machinery and equipment n.e.c.	IMPORTANT	IMPORTANT	NOT IN SCOPE
	Motor vehicles, trailers and semi-trailers	IMPORTANT	IMPORTANT	NOT IN SCOPE
	Other transport equipment	IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>DIGITAL PROVIDERS</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
<b>RESEARCH</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE

## Size-cap

### Definition of SME in NIS2



### 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 at **group level**:

- Large entity
- Medium entity
- Micro & Small entity

**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>

## Supervision mechanisms

Mechanism	To be sent to ILR	Essential entity	Important entity
Ex-ante	Security measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ex-post	Incident notification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ex-post	After incident & upon request	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



## Classification Scheme

Depending on sector & group-size of the entity.

For large & medium-sized entities:

- Essential entity
- Important entity

## Self-registration process!!

### > NISS

- > Nos missions
- > Législation
- > Décisions et règlements ILR
- > SERIMA (SEcurity Risk Management)
- > Mesures de sécurité
- > Notification d'incidents
- > Consultations
- > Directive NIS2



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

OVERVIEW OF CHANGES NIS2 IS BRINGING  
→ Governance & Security Measures





Cybersecurity as a Top Management Priority



Cybersecurity risk-management measures



Supply Chain Cybersecurity

RISK MANAGEMENT



## Management bodies need to:

- approve the cyber security measures;
- follow training in cybersecurity;
- offer similar training to employees.

## Policies

- Risk analysis & information security;
- Incident handling;
- Business continuity: backup management, disaster recovery & crisis management;
- Security in procurement: vulnerability handling & disclosure;
- Training & hygiene;
- Human resources & access control





## Supply Chain Cybersecurity

- **Security risks** between **entities** and their **suppliers** as well as their **service providers**
- Entities need to **assess the overall quality** of the cybersecurity practices of their suppliers and service providers by:
  - the cybersecurity of their **data storage** solutions
  - the cybersecurity of their **processing services**
  - the cybersecurity of their **security services**
- Vulnerability to cross-border cyber-threats



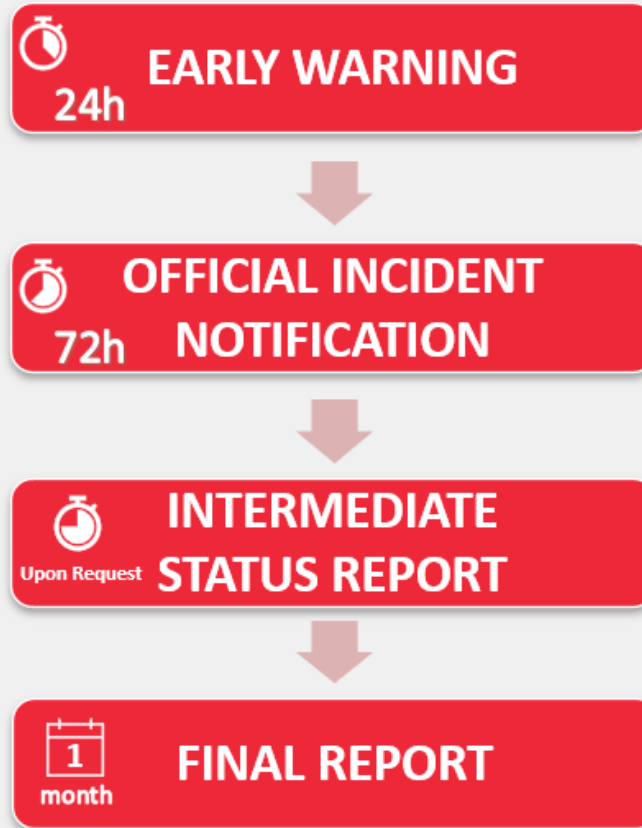
ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

OVERVIEW OF CHANGES NIS2 IS BRINGING  
→ Incidents & Information exchange







## Cybersecurity information-sharing arrangements

- Exchange between entities on a voluntary basis on:
  - cyber threats
  - near misses
  - Vulnerabilities
  - ...
- Enable information exchange within **communities of essential and important entities**, and possibly suppliers or service providers.
- Member States facilitate the **establishment** of information sharing arrangements.
- Entities notify the competent authority of their participation in such arrangements.

## Voluntary notification of relevant information

- Essential, important and other entities to notify:
  - Incidents, threats and near misses

## Good to know!

- CSIRT Tasks
  - Coordinated Vulnerability Disclosure mechanism & European Database
  - Implementing Acts by European Commission:
    - Incident notification
    - Security measures
- } for DNS, MSP, MSSP, TLD,  
Cloud, Data center, CDN, ...
- Peer Review
  - Mutual Assistance



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

OVERVIEW OF CHANGES NIS2 IS BRINGING  
→ Supervision mechanisms by authorities



## Competent Authority can:

- Do audits, inspections, request information,...
- And:
  - Issue warnings
  - Binding instructions
  - Order entities to inform their customers of cyber threats
- If enforcement ineffective:
  - Suspend temporarily certification or authorisation of relevant services
- Sanction

**Important!**

**Sanctions are not due to an incident occurring!**

## Administrative sanctions

In case of **non-compliance**:

- **Essential entities** face a fine of up to **€ 10 million** or **2%** of global annual turnover
- **Important entities** face a fine of up to **€ 7 million** or **1,4%** of global annual turnover  
whichever of the two is higher.



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

## ILR'S APPROACH





ILR's approach



Collaborative Approach



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



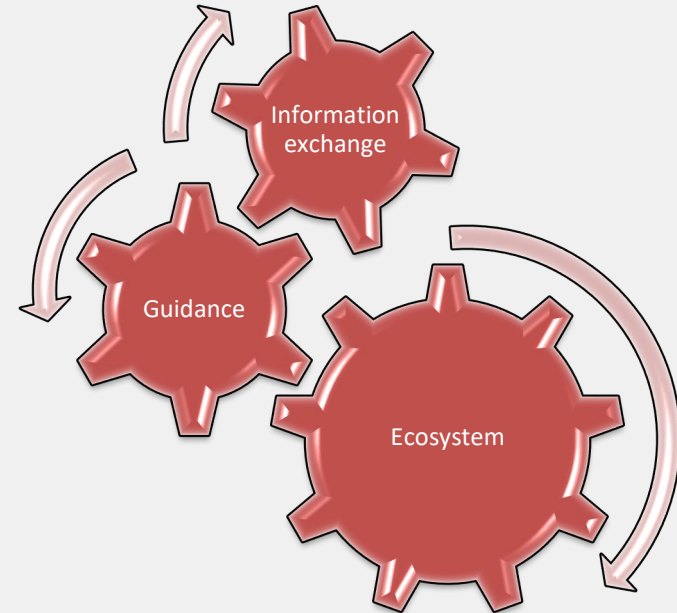


## Establish the key values:

- Information;
- Awareness;
- Collaboration.

## In order to:

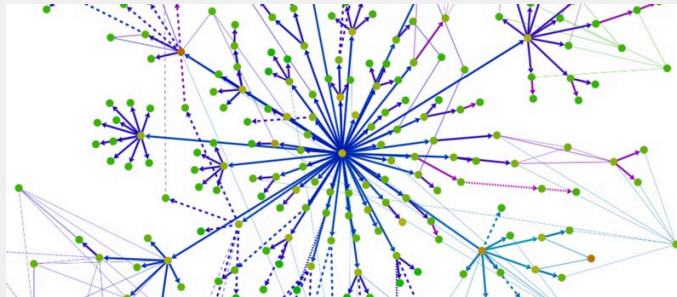
- Create an ecosystem;
- Promote information exchange within and among sectors;
- Establish guidance where needed in collaboration with the ecosystem.



## 1. Obligations for operators of essential services (OES)

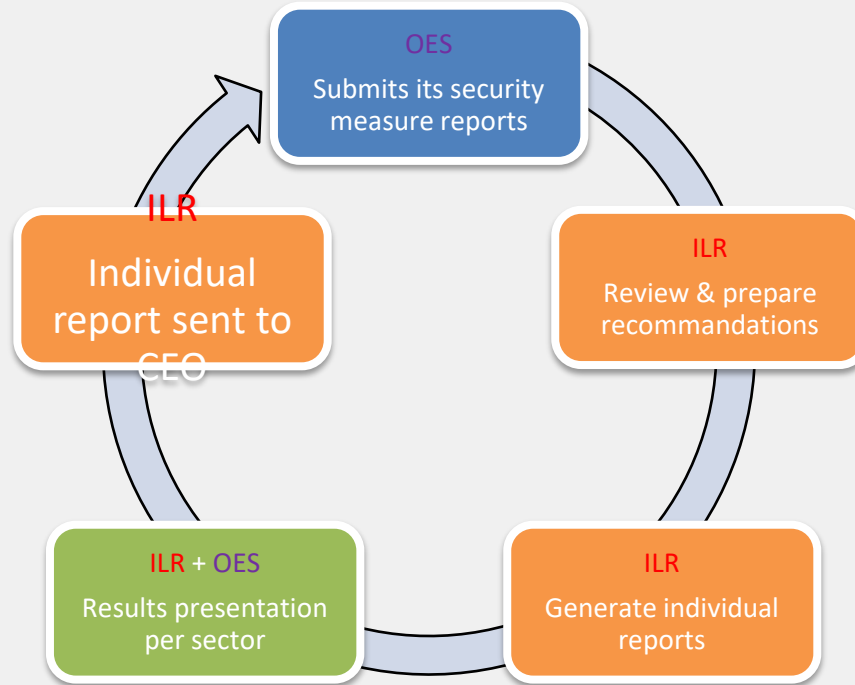
Règlement ILR/N22/7 du 15 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les opérateurs de services essentiels - NISS.

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



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)

# 1. Feedback cycle





## 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



Incident notification  
Ref. NIS\_IN191

Help

Step

Introduction	
Contact	
Preliminary notification	▼

Introduction

The operators have to notify their National Regulatory Authority (NRA) in case of incident having a significant impact on essential services and affecting networks or information systems. The notification happens in at least two steps:

- The operator has to fill a preliminary notification within 24 hours after having discovered the incident.
- The operator then needs to fill a complete notification after maximum 15 days of the preliminary notification. Or, in case the incident would be insignificant, to notify it to the ILR within the same timeframe.
- If after the final notification new important information is discovered by the operator, he has to submit an additional notification during 2 months of the final notification. An additional notification is basically an update of the final notification.

NEXT STEP >



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION


---

## SPECIFIC CHANGES DUE TO NIS2





## Risk Assessment

Risk Assessment on:	With NIS1	With NIS2	
Entity level		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Services delivered / sold		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Essential services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



## Security Objectives

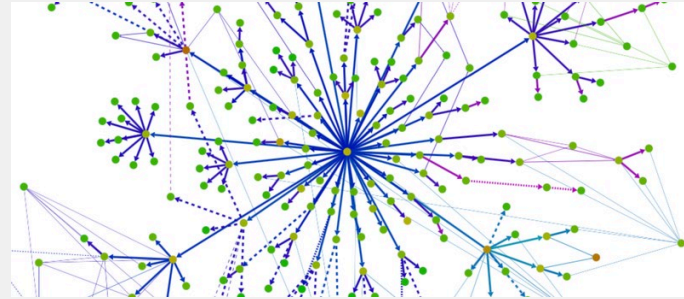
- Mapping between NIS2 and Security Objectives
- Addition of specific questions on:
  - C-level training
  - Internal audit
  - Backup

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)



## Dependencies

- Update of the template to include:
  - List of suppliers (not only essential);
  - Identify quality of products;
  - Vulnerabilities.



<i>Secteur &amp; Sous-secteur</i>	<i>Service Essentiel</i>	<i>Nom du fournisseur</i>	<i>Fournisseur étranger</i>	<i>Commentaire</i>



## CEO approval

Template to allow CEO to approve an executive summary for

- Risk assessment with the treatment plan
- Security Objectives
- Dependencies





ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

# TIMELINE FOR IMPLEMENTATION OF NIS2



# ILR TIMELINE



## NIS 2 Information sessions

Q4 2023 & Q1 2024



## NISDUC Conference

23-24. April 2024



## Guidelines on risk assessment

Mid 2024



## New Dependencies Template

Mid 2024



## Updates ILR Regulations

After 17. October 2024



## NIS 2 National Transposition

17. October 2024



## Guidelines on security policies

Mid 2024



## Self-registration of entities

17. January 2025



## List of essential and important entities

17. April 2025



ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

## **COLLABORATION & SUPPORT BY ILR**





ILR

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](http://www.ilr.lu)

