



ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

NIS2 Directive and its challenges

Sheila Becker



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



ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

OVERVIEW OF CHANGES NIS2 IS BRINGING





- **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
 POSTAL & COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
 WASTE MANAGEMENT		IMPORTANT	IMPORTANT	NOT IN SCOPE
 MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS		IMPORTANT	IMPORTANT	NOT IN SCOPE
 PRODUCTION, PROCESSING AND DISTRIBUTION OF FOODS		IMPORTANT	IMPORTANT	NOT IN SCOPE
 MANUFACTURING	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
 DIGITAL PROVIDERS		IMPORTANT	IMPORTANT	NOT IN SCOPE
 RESEARCH		IMPORTANT	IMPORTANT	NOT IN SCOPE



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"/>

Entités tombants sous NIS2 en tant que administration publique:

Conditions:

- Intérêt général;
- Personnalité juridique ou juridiquement habilitée;
- Financement avec moyens publics;
- Pouvoir adjudicateur.

Exceptions:

- Justice
- Chambre des députés
- BCL



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

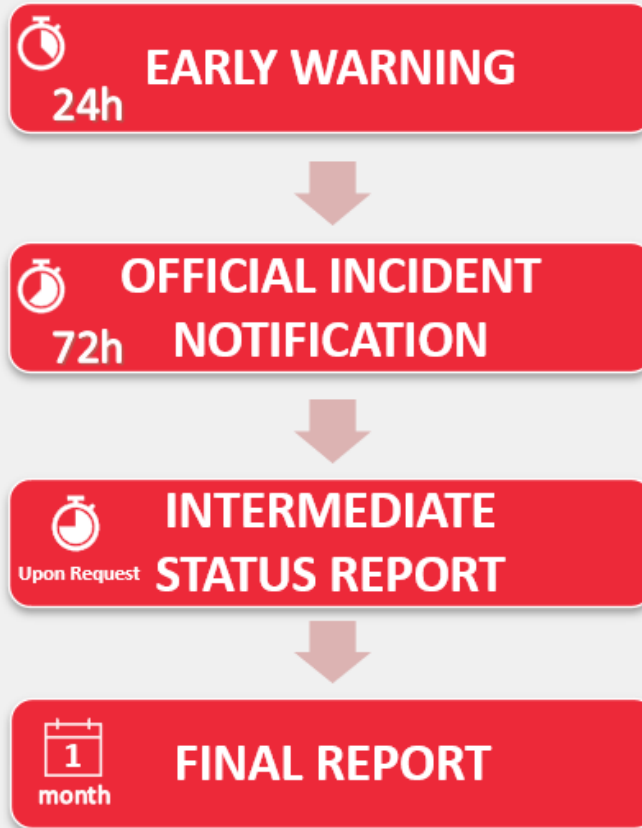


ILR

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



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





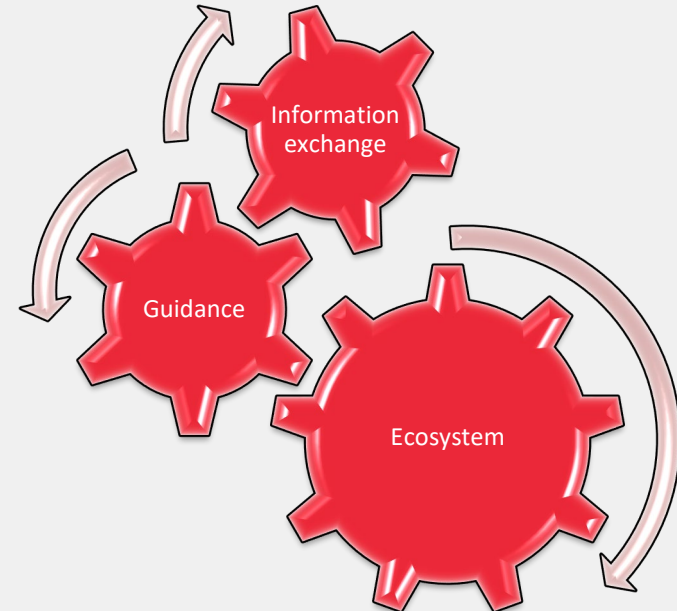


Establish the key values:

- Information;
- Awareness;
- Collaboration.

In order to:

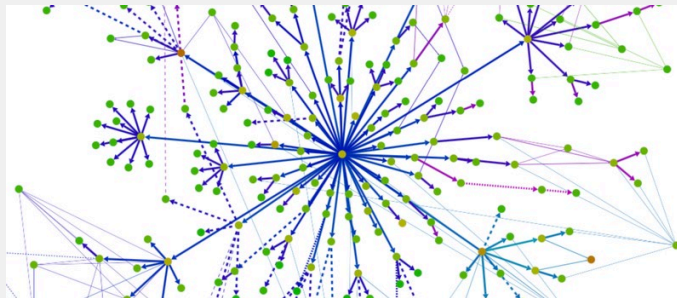
- Create an ecosystem;
- Promote information exchange within and among sectors;
- Establish guidance where needed in collaboration with the ecosystem.



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)

CEO approval

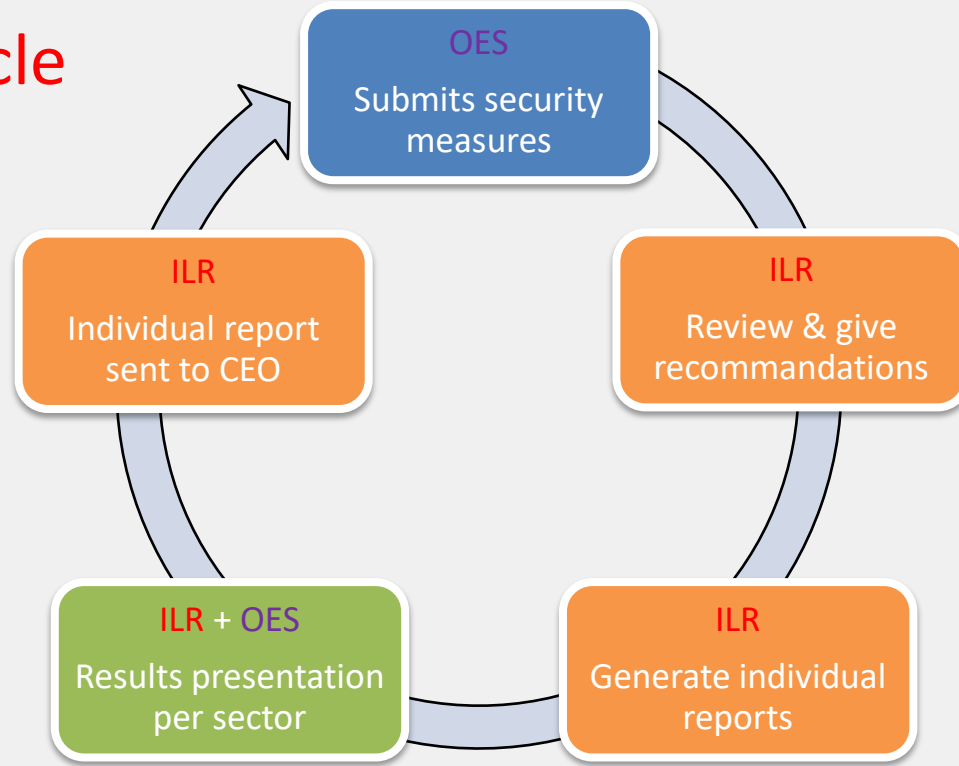
Template to allow CEO to approve an executive summary for

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



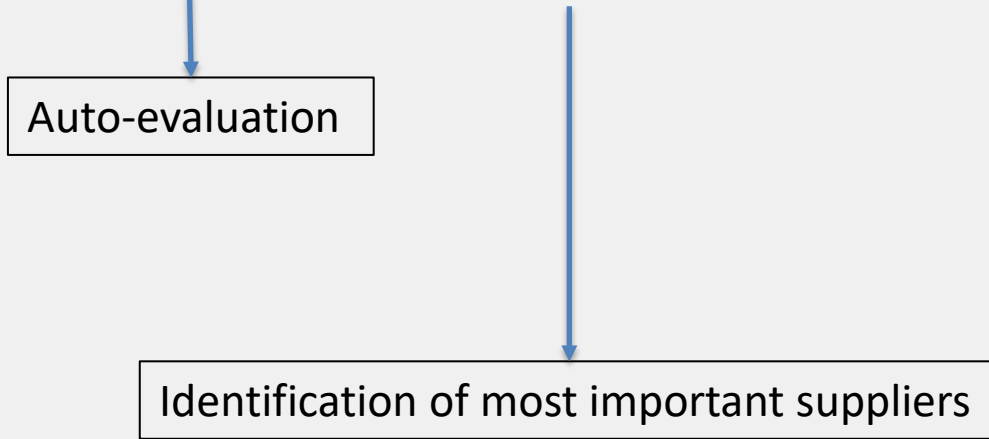


Feedback cycle



Starting point for new NIS2 & small entities

- Focus on security objectives & dependencies



- No Risk Assessment Obligation in the beginning



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

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

