




ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

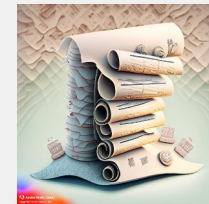
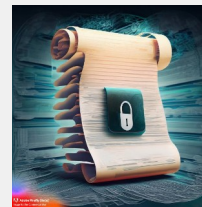
COLLABORATION, GUIDANCE AND SUPPORT FOR NIS2 ENTITIES

Presented by:

- **ILR** – Institut Luxembourgeois de Régulation
Jacques Kellner
 - **LHC** – Luxembourg House of Cybersecurity
Gérard Wagener
 - **LIST** – Luxembourg Institute of Science and Technology
Hervé Cholez
- 



Challenges from NIS to NIS 2



- 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

- Lack of Awareness for the NIS 2 Scope
- How and where to start for assessing and improving cybersecurity maturity?
- How to improve information exchange?
- Short timeline for transposition and implementation



INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

GLOBAL CYBERSECURITY PLATFORM



SERIMA.LU

Security Risk Management

Risk assessment



Perform a risk assessment to protect your most valuable assets

Incident notification



Notify your incidents to ILR

Security objectives



Fill the questionnaire with the security objectives to self-assess your security level

Dependencies



Know your suppliers that you depend on to provide your services to your customers

Incident notification platform

- **Multi-regulation**



- **Completely configurable:**

- Reports

EARLY WARNING

- Questions

OFFICIAL INCIDENT
NOTIFICATION

- Deadlines

INTERMEDIATE
STATUS REPORT

FINAL REPORT

- **Review by authorities on the platform**



Enter your credentials.

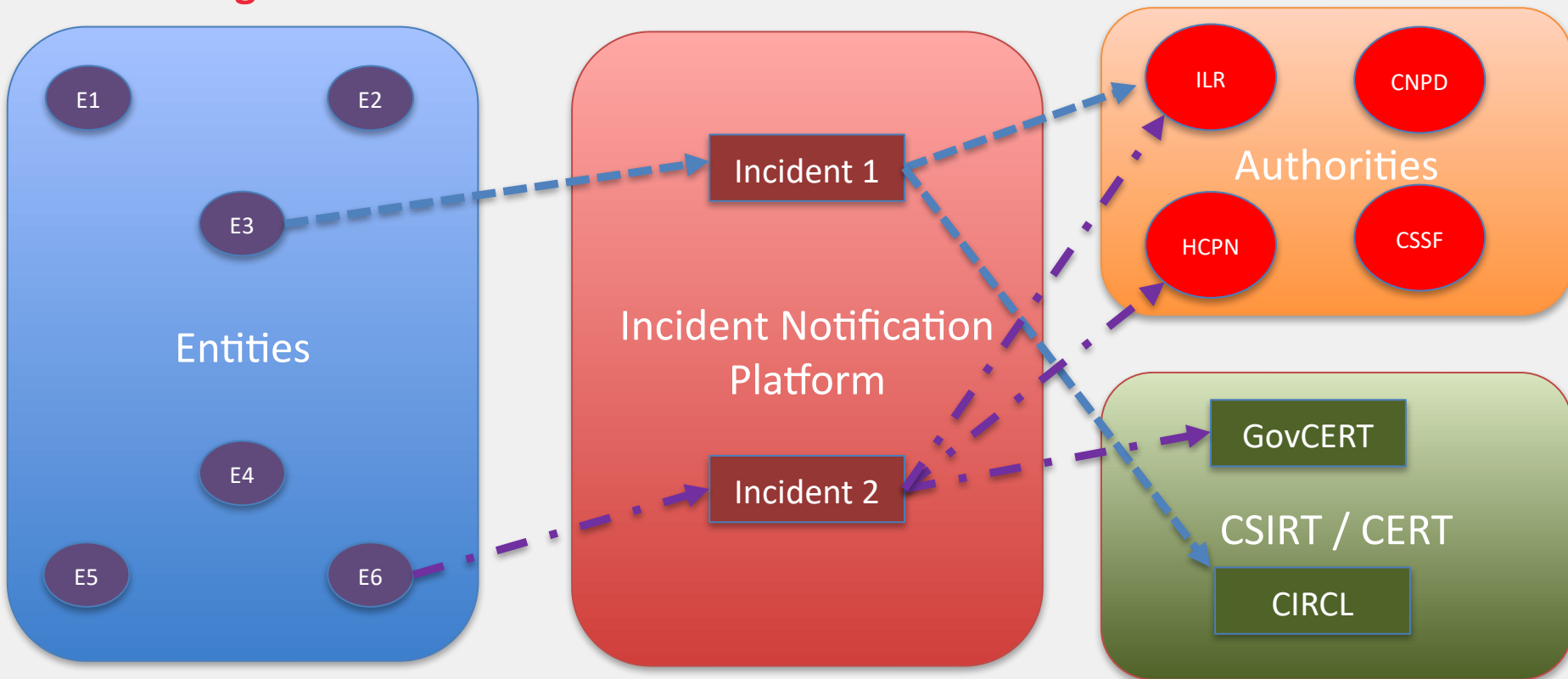
Log in

[Forgotten your password or username?](#)

No account and need to notify an
incident ?

[Sign Up](#)

Multi-regulator





INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

GUIDELINES

Guidelines

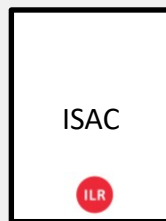
General Guidelines

- Adapted to the maturity of a company in regards to cybersecurity



- Size of a company matters
- Sectoral specifications – Dependence on digital elements matters

Subject specific Guidelines





INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

AWARENESS RAISING

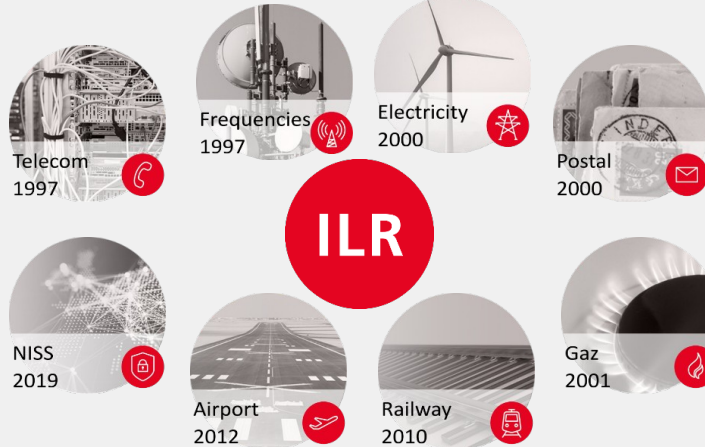


Approach

Information sessions
Conferences & local



Contacting regulated entities



collaborations





ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

LIST OF ESSENTIAL AND IMPORTANT ENTITIES IN LUXEMBOURG

Hervé Cholez (LIST)

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY



Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities:

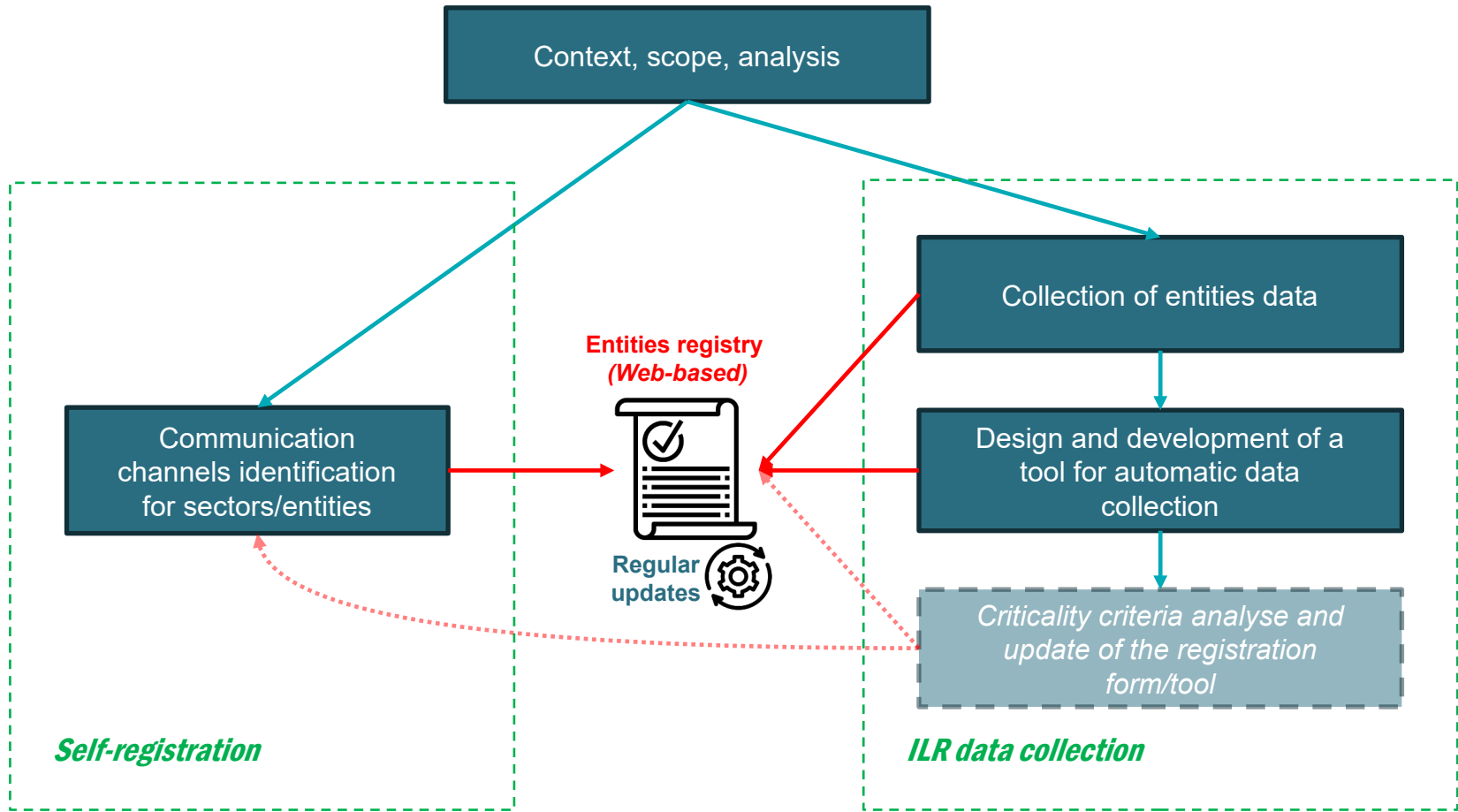


(a) the **name** of the entity

(b) the **address** and up-to-date **contact details**, including email addresses, IP ranges and telephone numbers

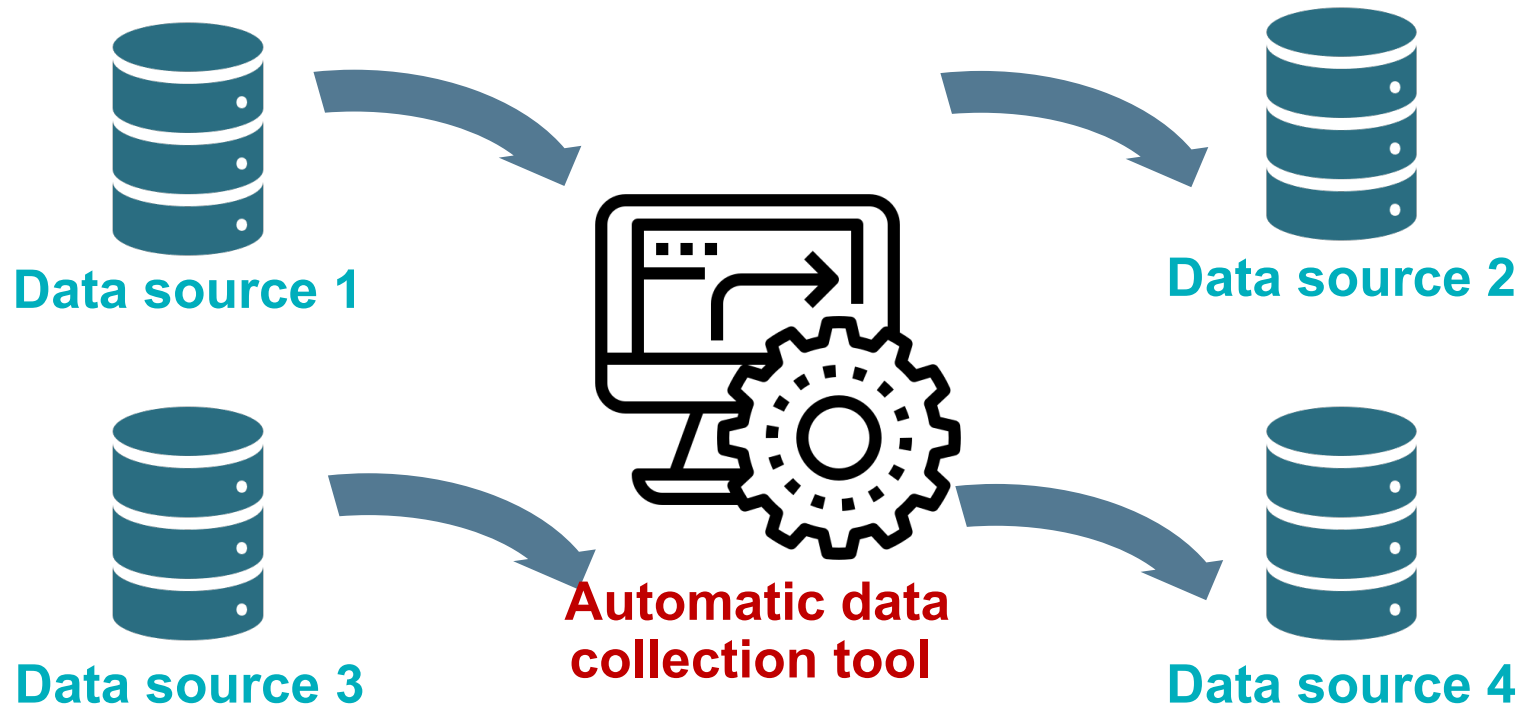
(c) where applicable, the **relevant sector and subsector** referred to in Annex I or II

(d) where applicable, a list of the **Member States where they provide services** falling within the scope of this Directive



support activities in Luxembourg

Data collection





ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

COLLABORATION - VULNERABILITY DISCLOSURE

Gérard Wagener (CIRCL)



circl.lu
Computer Incident
Response Center
LUXEMBOURG

Current vulnerabilities disclosure activities

- Vital for enhancing IT security.
- Often neglected despite its importance.
- Case study: A pentester discovers a vulnerability in Product X.
 - Pentester informs the client.
 - Client opts to discontinue the product.
 - Vulnerability remains unreported to the vendor due to lack of resources.
 - CIRCL offers anonymous vulnerability reporting services.
 - CIRCL takes the workload of vulnerability disclosure.
 - CIRCL issues technical reports with details and remedies for vulnerabilities affecting a significant portion of the constituency.

What does vulnerability disclosure work involve?

- Engagement with the reporter.
- Evaluation of the claim:
 - Reproducibility, duplication, nature, etc.
 - Request for standardized referencing in national and international databases like those managed by [CVE](#).
- Collaboration with the vendor:
 - Confirmation of vulnerability resolution and publication.
- Communication with relevant local stakeholders such as NC3, ILR, and the general public to relay the vulnerability.

What will be new in NIS2 regarding at CIRCL vulnerability disclosure

- NIS2 reinforces the legal framework of vulnerability reporting.
- NIS2 will boost incentives to report vulnerabilities.
- CIRCL will provide new tooling for vulnerability management.
- Scenario-based Cyber Security Incident for risk assessment:
 - will be open data
 - can be used by regulators
 - can be use by observatory
 - New tooling available: <https://github.com/cve-search/vulnerability-lookup>

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



INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

Thank you!
Any questions?

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