



**SERIMA**.LU

Security Risk Management  
Powered by ILR

# GLOBAL CYBERSECURITY PLATFORM

Sascha MAURER  
Service NISS

May 19th 2026



INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

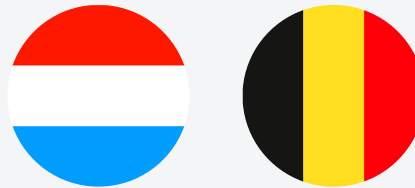
<b>01. SERIMA as a Global Cybersecurity-Platform</b>	3
<b>02. Incident Notification Module</b>	11
<b>03. Security Objectives Module</b>	17
<b>04. Development Roadmap &amp; Outlook</b>	23
<b>05. Q&amp;A</b>	28

# 01. SERIMA as a Global Cybersecurity-Platform



# The national cybersecurity platform of Luxembourg for **NIS 2**

The SERIMA platform is the result of a **collaborative development** effort between **Luxembourg & Belgium**.





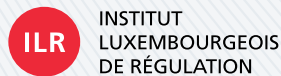
is a **joint development effort** between:



The Luxembourg House of Cybersecurity and its  
National Cybersecurity Competence Center



The Belgian Institute for Postal Services and  
Telecommunications





The Luxembourgish Institute for Regulation




# 01. A Global Cybersecurity-Platform

**1**   
**OPEN SOURCE**  
Transparent, independent,  
and cost-effective

**2**   
**COLLABORATIVE**  
Created and improved by a  
dedicated community

**3**   
**COMMITMENT**  
Sustaining and growing the  
solution together

**4**   
**CONFIGURABLE**  
Tailored workflows for evolving  
administrative requirements



## 6 Key Functional Principles



### **SYSTEM ADAPTABILITY**

Modeling workflows, deadlines, and standards for specific requirements.



### **ADMINISTRATIVE SIMPLIFICATION**

Centralized with guided processes to streamline administrative workflows



### **CENTRALIZED OVERSIGHT**

Track deliverables, submission statuses, and multi-year data comparability



### **COLLABORATIVE EXCHANGE**

Structured bidirectional communication and integrated feedback loops



### **REPORTING & DOCUMENTATION**

Generating standardized reports and audit logs



### **MULTILINGUAL**

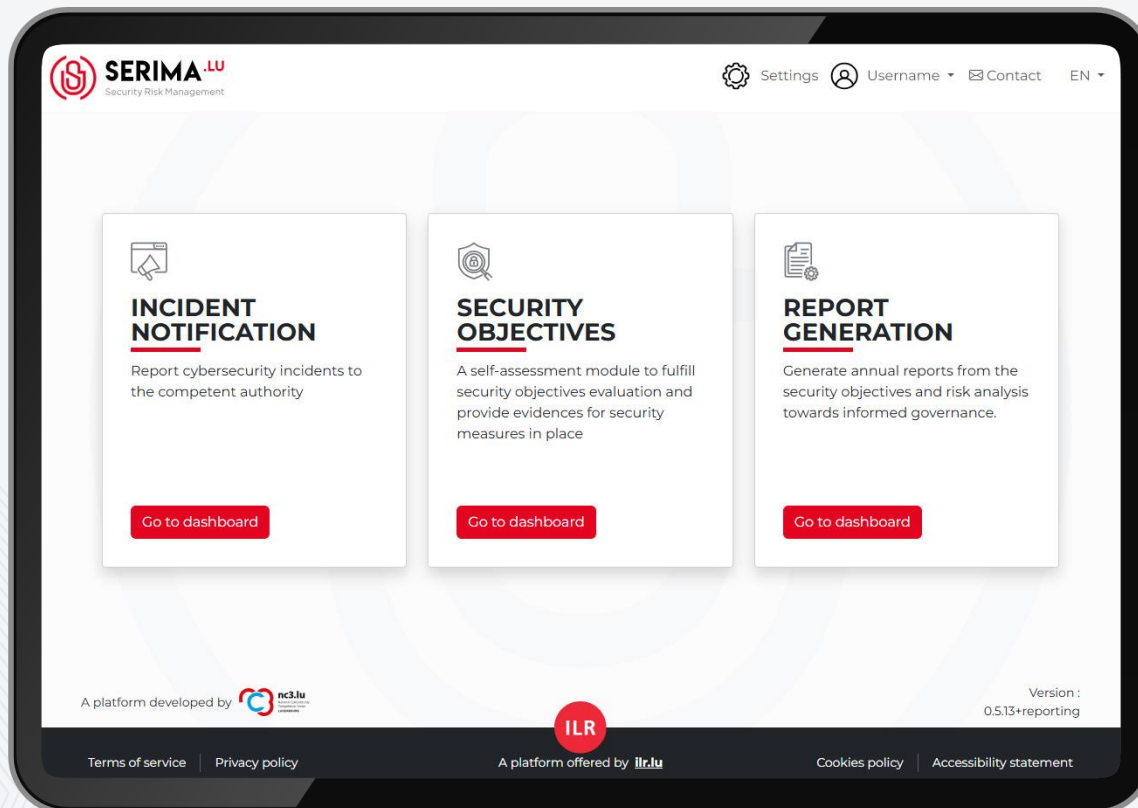
Interface and helpdesk in English, French and German



is not a regulatory constraint,  
but a tool for **administrative simplification**

⇒ SERIMA is a strategic enabler for  
**informed governance**

# 01. A Global Cybersecurity-Platform

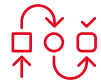


# 02. Incident Notification Module

# Module Features



**Centralized Repository**



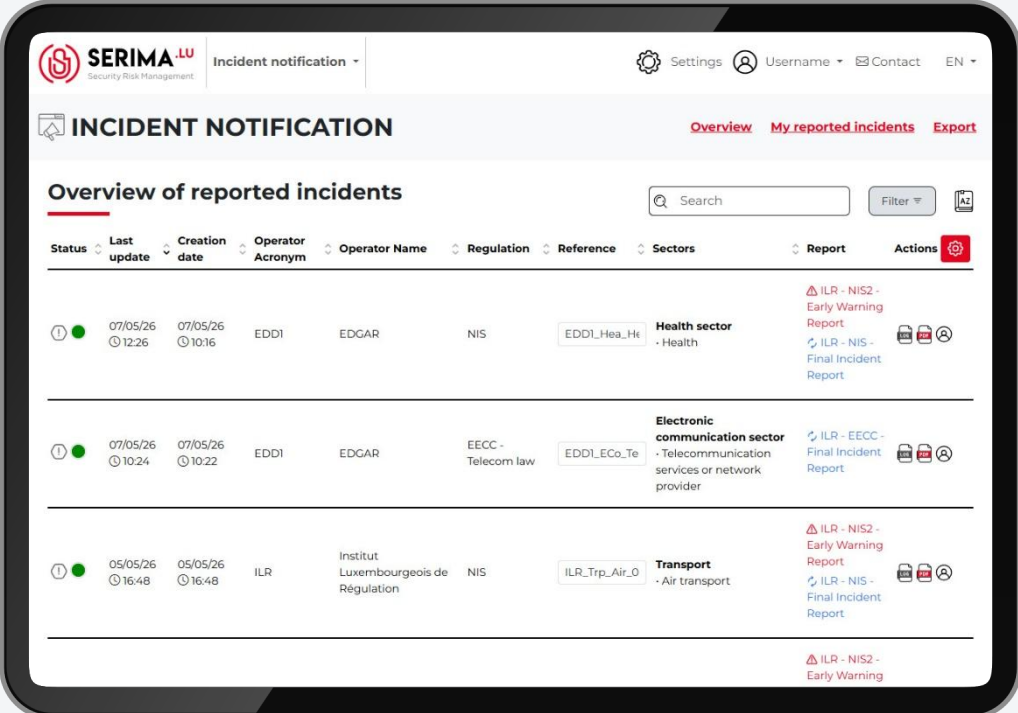
**Guided Workflow**



**Configurable Module**



**Simplified Compliance**















**SERIMA**.LU Security Risk Management Incident notification - Settings Username Contact EN

### INCIDENT NOTIFICATION

Overview My reported incidents Export

#### Overview of reported incidents

Search Filter

Status	Last update	Creation date	Operator Acronym	Operator Name	Regulation	Reference	Sectors	Report	Actions
 	07/05/26 🕒 12:26	07/05/26 🕒 10:16	EDDI	EDGAR	NIS	EDDI_Hea_He	<b>Health sector</b> - Health	<a href="#">ILR - NIS2 - Early Warning Report</a> <a href="#">ILR - NIS - Final Incident Report</a>	 
 	07/05/26 🕒 10:24	07/05/26 🕒 10:22	EDDI	EDGAR	EECC - Telecom law	EDDI_ECo_Te	<b>Electronic communication sector</b> - Telecommunication services or network provider	<a href="#">ILR - EECC - Final Incident Report</a>	 
 	05/05/26 🕒 16:48	05/05/26 🕒 16:48	ILR	Institut Luxembourgeois de Régulation	NIS	ILR_Trp_Air_0	<b>Transport</b> - Air transport	<a href="#">ILR - NIS2 - Early Warning Report</a> <a href="#">ILR - NIS - Final Incident Report</a>	 

[ILR - NIS2 - Early Warning](#)

# Module Features



**Centralized** Repository



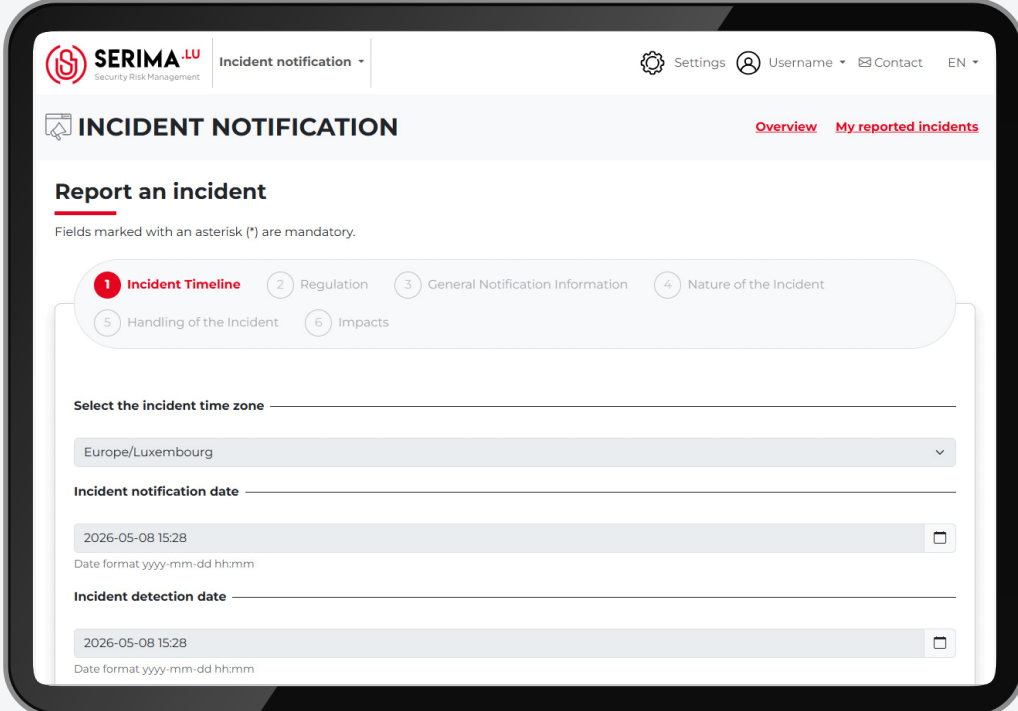
**Guided** Workflow



**Configurable** Module



**Simplified** Compliance

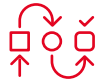


The screenshot displays the 'Incident notification' interface within the SERIMA .LU system. The header includes the SERIMA .LU logo and 'Security Risk Management', along with navigation options for 'Settings', 'Username', 'Contact', and 'EN'. The main heading is 'INCIDENT NOTIFICATION', with links for 'Overview' and 'My reported incidents'. The primary action is 'Report an incident', with a note that fields marked with an asterisk (\*) are mandatory. A progress indicator shows six steps: 1. Incident Timeline (active), 2. Regulation, 3. General Notification Information, 4. Nature of the Incident, 5. Handling of the Incident, and 6. Impacts. The form includes a 'Select the incident time zone' dropdown menu currently set to 'Europe/Luxembourg', and two 'Incident notification date' and 'Incident detection date' fields, both pre-filled with '2026-05-08 15:28' and a date format hint 'Date format yyyy-mm-dd hh:mm'.

# Module Features



**Centralized** Repository



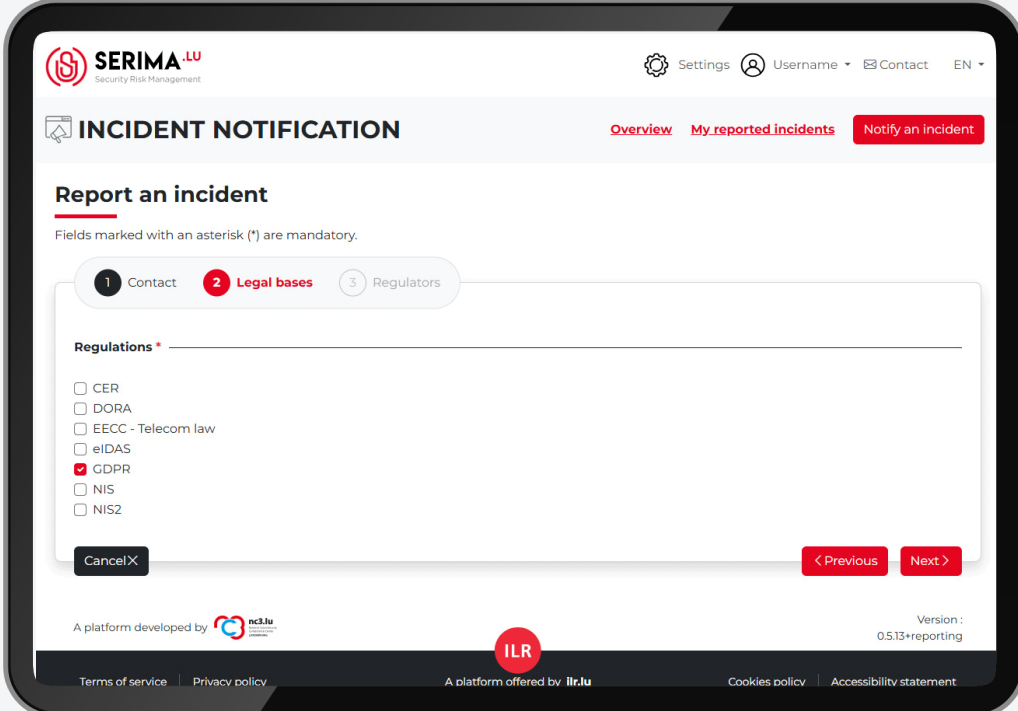
**Guided** Workflow



**Configurable** Module



**Simplified** Compliance



**SERIMA .LU** Security Risk Management

Settings Username Contact EN

### INCIDENT NOTIFICATION

Overview My reported incidents **Notify an incident**

#### Report an incident


Fields marked with an asterisk (\*) are mandatory.

1 Contact 2 **Legal bases** 3 Regulators

**Regulations \***


- CER
- DORA
- EEC - Telecom law
- eIDAS
- GDPR**
- NIS
- NIS2

CancelX **< Previous** **Next >**

A platform developed by  nc3.lu

Version : 0.513+reporting

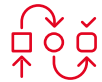
**ILR**

Terms of service | Privacy policy | A platform offered by  ilr.lu | Cookies policy | Accessibility statement

# Module Features



**Centralized** Repository



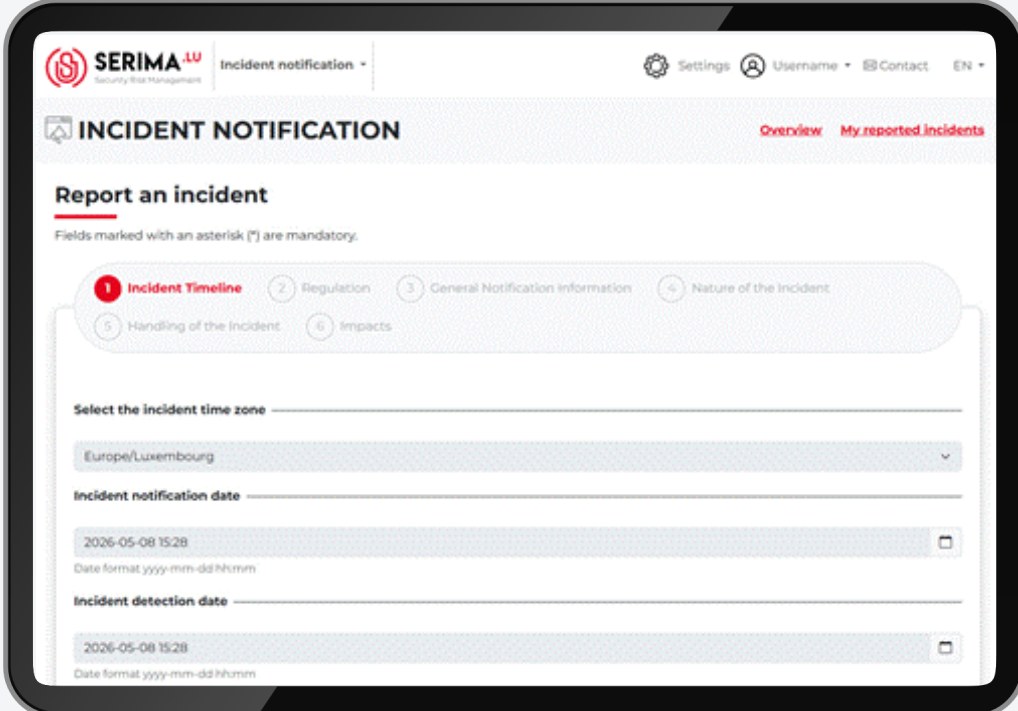
**Guided** Workflow



**Configurable** Module



**Simplified** Compliance



The screenshot displays the 'INCIDENT NOTIFICATION' interface within the SERIMA .LU application. The header includes the SERIMA .LU logo, the text 'Incident notification', and navigation links for 'Settings', 'Username', 'Contact', and 'EN'. Below the header, there are links for 'Overview' and 'My reported incidents'. The main section is titled 'Report an incident' and includes a note: 'Fields marked with an asterisk (\*) are mandatory.' A progress bar shows six steps: 1. Incident Timeline (active), 2. Regulation, 3. General Notification information, 4. Nature of the Incident, 5. Handling of the Incident, and 6. Impacts. The form contains three input fields: 'Select the incident time zone' (with a dropdown menu showing 'Europe/Luxembourg'), 'Incident notification date' (with a date picker showing '2026-05-08 15:28'), and 'Incident detection date' (with a date picker showing '2026-05-08 15:28').

## Incident Notification Workflow - NIS 2

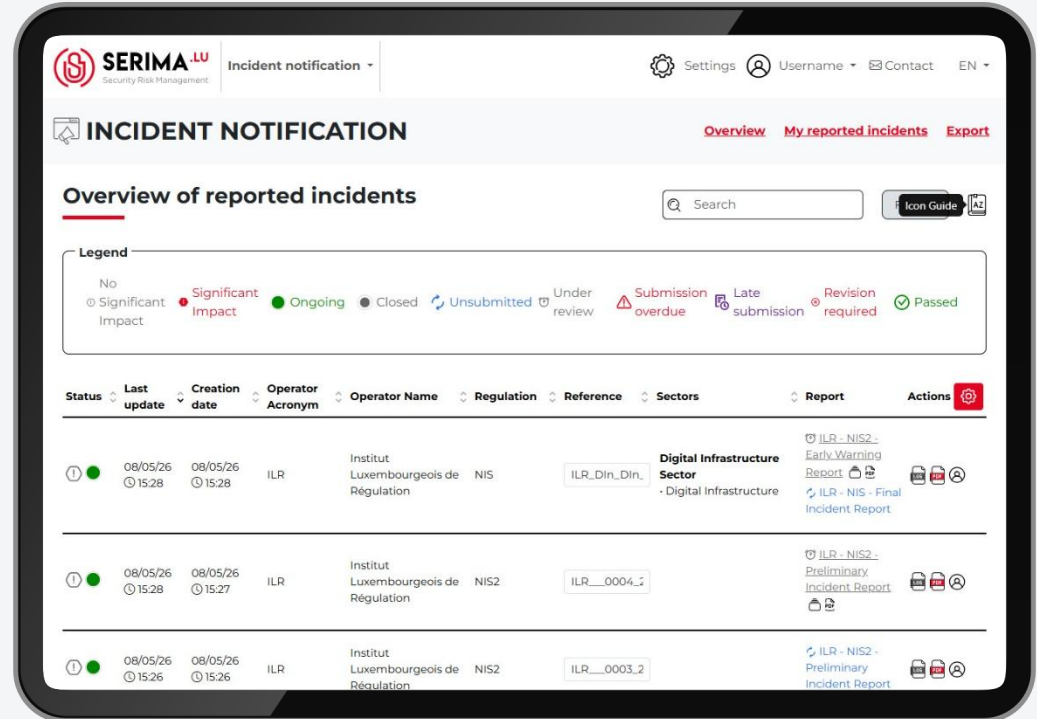


**EARLY WARNING**

**OFFICIAL INCIDENT NOTIFICATION**

**OFFICIAL INCIDENT NOTIFICATION**

**FINAL REPORT**



# 03. Security Objectives Module

## Module Features



Centralized Repository



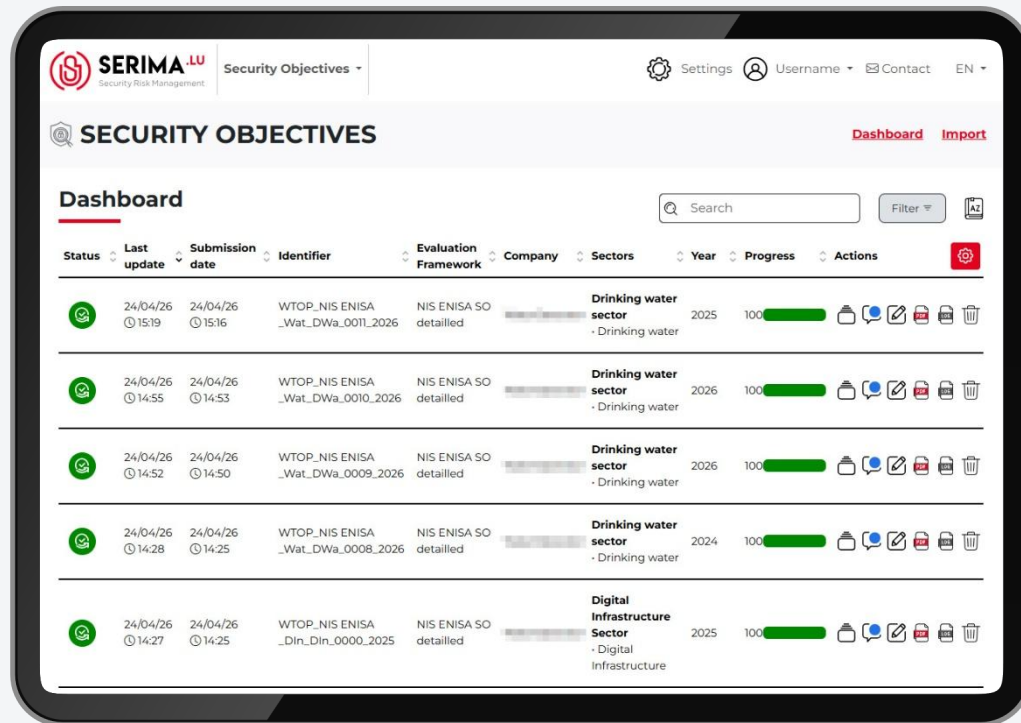
Iterative Workflow



Configurable Module



Cyber Maturity Assessment



## Module Features



Centralized Repository



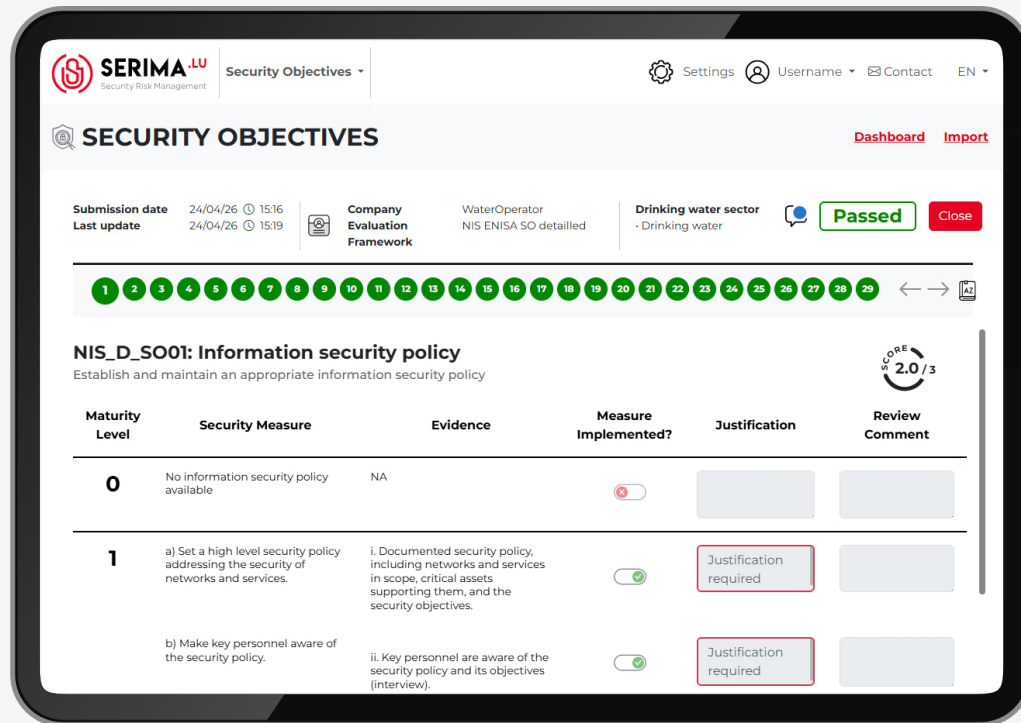
Iterative Workflow



Configurable Module



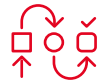
Cyber Maturity Assessment



## Module Features



Centralized Repository



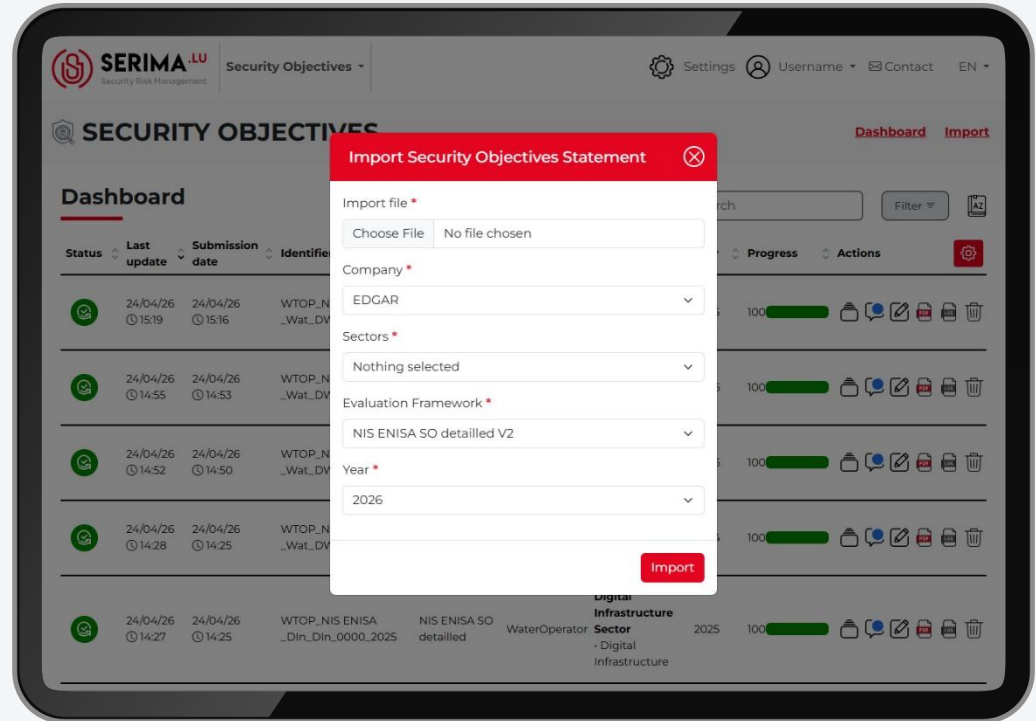
Iterative Workflow



Configurable Module



Cyber Maturity Assessment



## Module Features



Centralized Repository



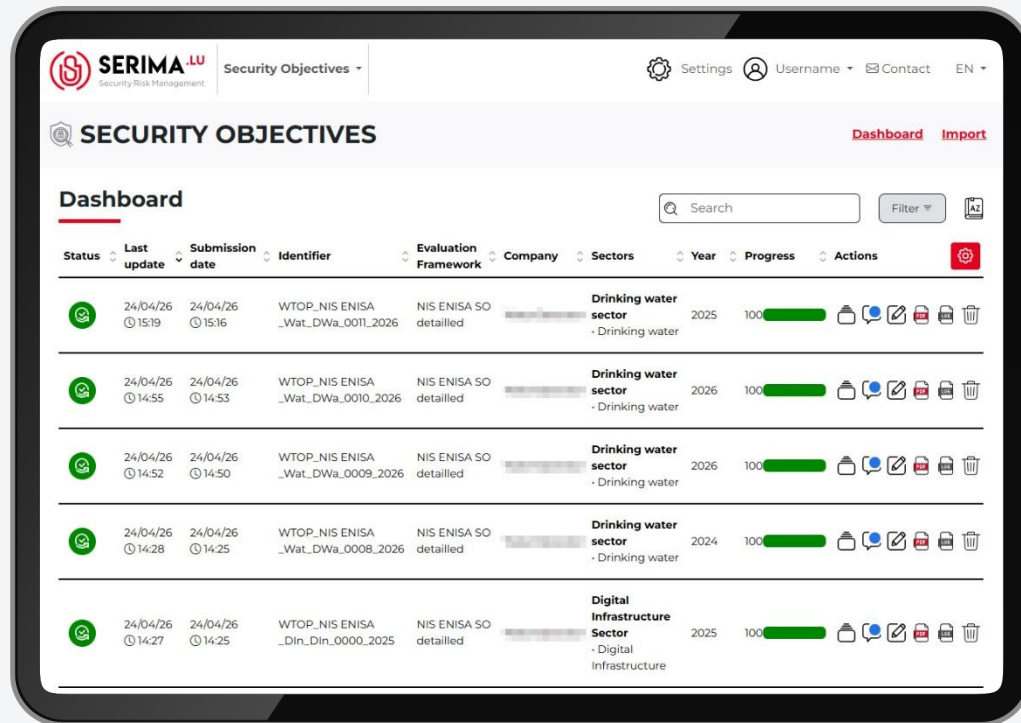
Iterative Workflow



Configurable Module



Cyber Maturity Assessment



## Security Objectives Workflow - NIS 2



Evidence-Based Maturity Assessment

Identify areas of improvement

Give & receive feedback

Benchmark, Decide, Repeat

The screenshot shows the SERIMA LU Security Objectives interface. At the top, it displays the SERIMA LU logo and 'Security Objectives' dropdown. On the right, there are links for 'Settings', 'Username', 'Contact', and 'EN'. Below this, the main heading is 'SECURITY OBJECTIVES' with 'Dashboard' and 'Import' links. A summary bar shows 'Submission date' and 'Last update' as 24/04/26 at 15:16 and 15:19 respectively, 'Company Evaluation Framework' as 'WaterOperator NIS ENISA SO detailed', and 'Drinking water sector' as 'Drinking water'. A green 'Passed' button and a red 'Close' button are visible. A progress bar with 29 numbered steps is shown, with step 1 highlighted. Below this, the objective is 'NIS\_D\_SO01: Information security policy' with a description 'Establish and maintain an appropriate information security policy' and a 'SCORE 2.0 / 3' indicator. A table follows with columns for 'Maturity Level', 'Security Measure', 'Evidence', 'Measure Implemented?', 'Justification', and 'Review Comment'. The table shows two rows for maturity level 1, with the first row having a 'Justification required' box and the second row also having a 'Justification required' box.

Maturity Level	Security Measure	Evidence	Measure Implemented?	Justification	Review Comment
0	No information security policy available	NA	<input type="checkbox"/>		
1	a) Set a high level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. ii. Key personnel are aware of the security policy and its objectives (interview).	<input checked="" type="checkbox"/>	Justification required	

# 04. Development Roadmap & Outlook

## 04. Development Roadmap & Outlook

### Incident notification

Report incidents to the competent authority

**Available**

### Security objectives

Assess your maturity level and identify areas of improvement

**BETA Testing**

### Entity Self-Registration\*\*

Self-register your entity if you fall under NIS2

**Development**

### Risk assessment\*

Perform a risk assessment to identify and protect your most valuable assets

**Available**

### Report Generation

Generate annual reports and receive feedback

**BETA Testing**

### C-level Approval Report

Approve your security measures as management body

**Development**

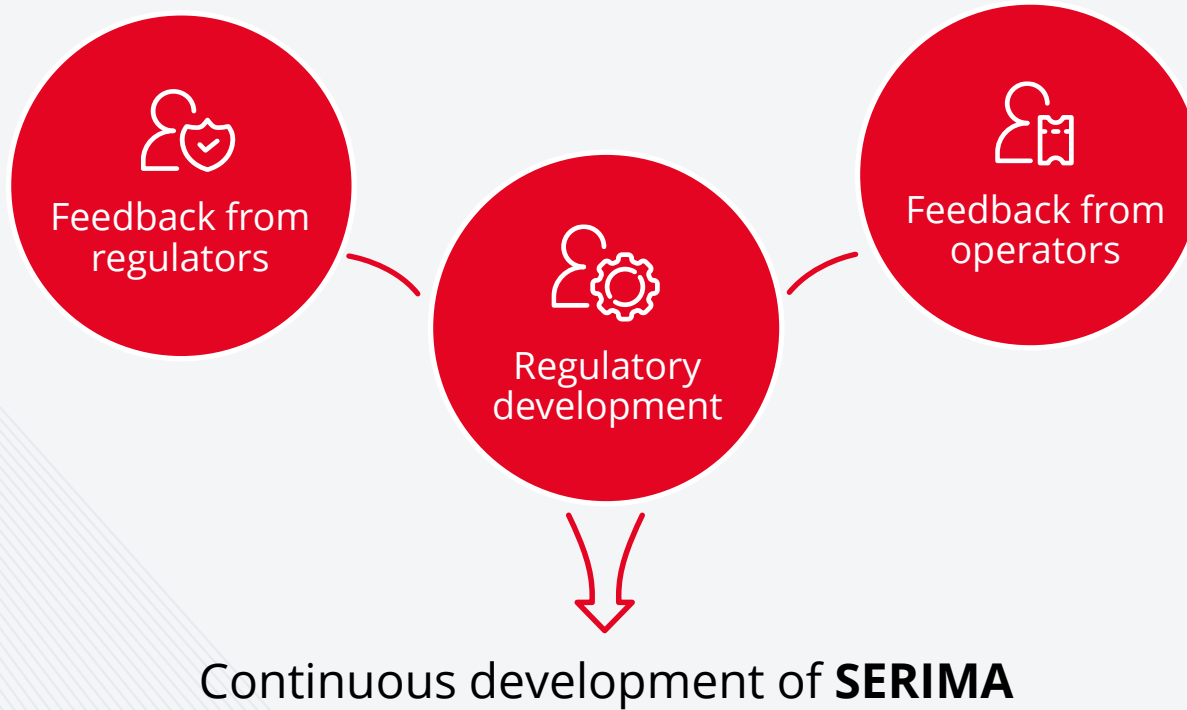
\* Based on the MONARC (asset based) technology

\*\* Self-Registration is currently possible through a separate online form in LU



**Development** for **several other modules** has already started:

- High-Level Risk Assessment (Scenario-Based)
- Action Plan
- Dependencies





Leveraging **administrative simplification**  
to enable  
**informed governance.**

# Questions ?

Join the SERIMA community!

 [serima@ilr.lu](mailto:serima@ilr.lu)



**SERIMA**.LU

Security Risk Management

17, rue du Fossé  
Adresse postale  
L-2922 Luxembourg

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



**nc3.lu**

National Cybersecurity  
Competence Center  
LUXEMBOURG

**bipt**



Belgian Institute for Postal Services  
and Telecommunications

ILR

INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

ILR