

GLOBAL CYBERSECURITY PLATFORM

Jacques Kellner May 7th 2025





01. SE	RIMA as a Global Cybersecurity-Platform	3
<mark>02.</mark> In	cident Notification Module	7
02	2.01. Module Features	9
<mark>03.</mark> Ri	sk assessment Module	12
04. Se	ecurity Objectives Module	15
<mark>05.</mark> In	terplay of the Modules	17
<mark>06.</mark> Qi	uestions	19



01. SERIMA as a Global Cybersecurity-Platform



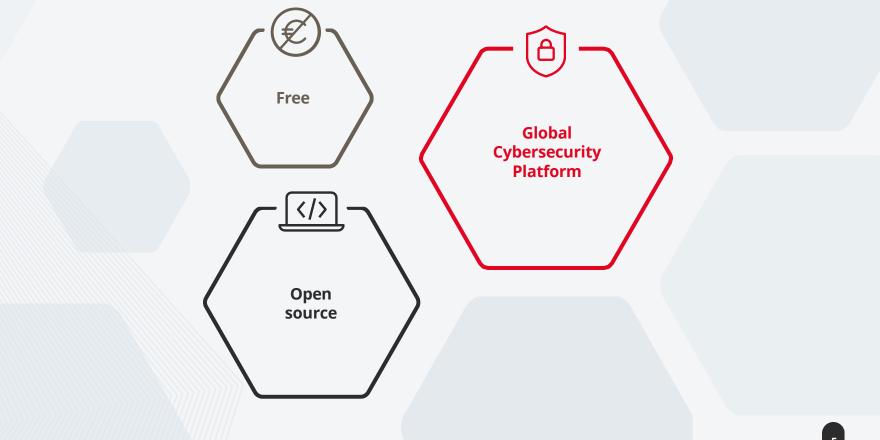
SERIMA – Main goals

- ILR Support for the community
- Tool to facilitate the activities regarding cybersecurity
- Centralisation of information to facilitate informed governance

01. SERIMA as a Global Cybersecurity-Platform

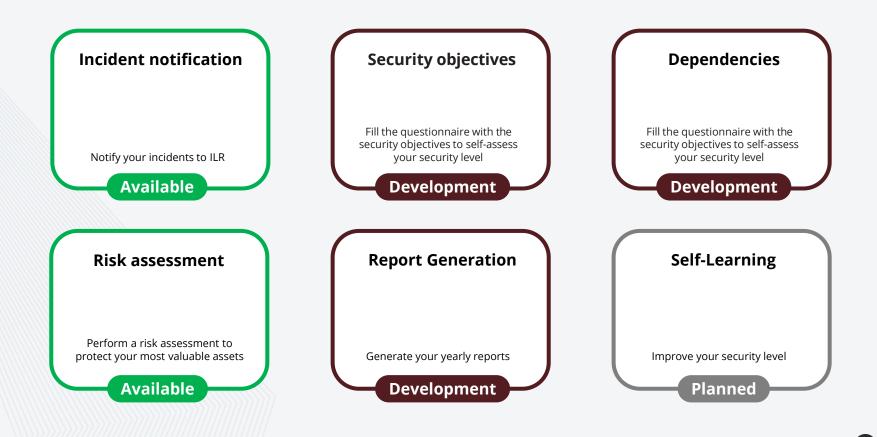






01. SERIMA as a Global Cybersecurity-Platform



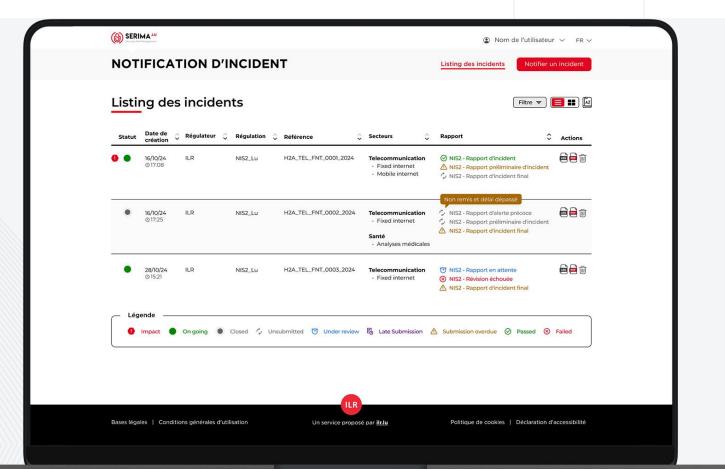




02. Incident Notification Module

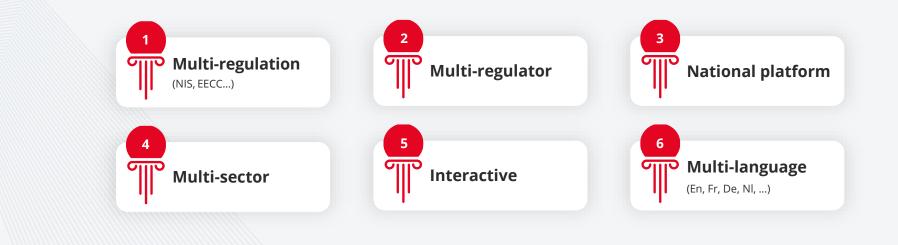
02. Incident Notification Module





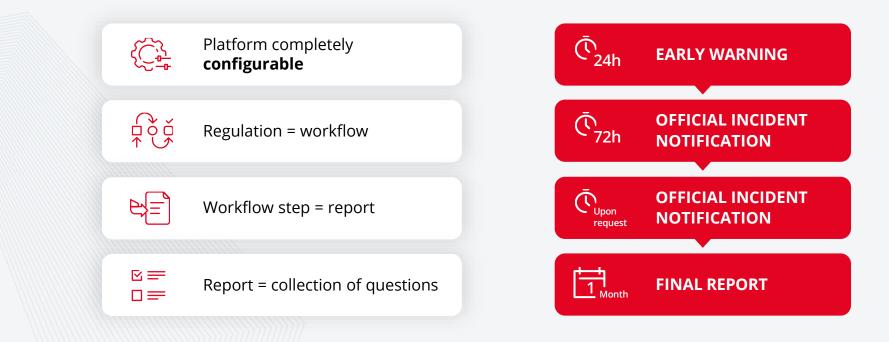


Incident Notification - 6 pillars



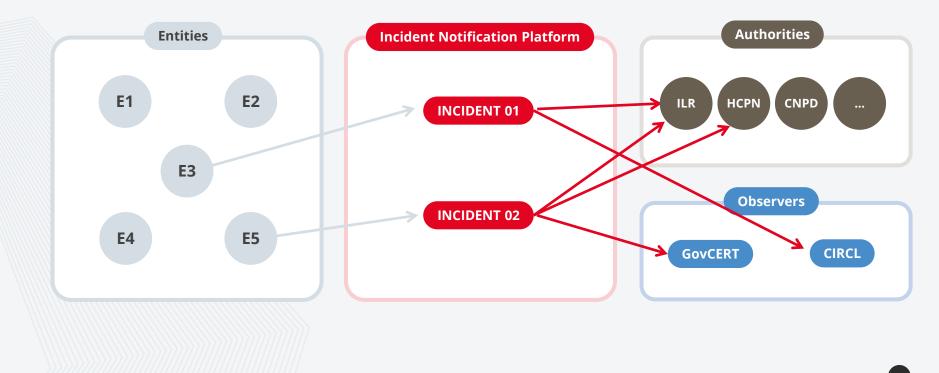


Multi-regulation





Multi-regulator





03. Risk assessment Module

03. Risk assessment module

Risk assessment

- Based on the MONARC Technology
- Sectoral librairies under NIS1 and EECC
- NIS2: Generic library + specific sectoral libraries







03. Risk assessment module





Home > My Analysis											¢ 1	- HE - E
		-8-		_		0-					_	(
sk analysis 🔗 🔿 Expand all 7 - Wieppall	HR Department Department as an entity that regroup persons Confidentiality: 3				Implementation and monitoring Availability: 1							
Search an ooset	Informati	on risks	Operational risks		Deliverable: Implementation Pla							
My Analysis + HR Department + Production Department 84 informati		mation risk:	B Risk threshold (on n	nax GIA) 🄇	C Keywards	Type de treitement 👻	۹ 🖸	ŧ	Sart MAD	K risk	* Descend	
sets library ^		Impact	Threat		Vu	Vulnerability		Current risk			- Resid	
Search an accel	Asset	C I A	Label	Prob.	Label	Existing controls	Qualif.	c	1	А	Treatment	risk
Fundamentals EBIOS	Administration workstations	3 1 1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
	Administrator	3 1 1	Lorging of rights	3	Authorisation management is flawed	No procedure	4		12	12	Reduction	e.
	Administrator	s 1 1	Malware mechan	2	Programs can be dewnloaded and installed without mentioning	Nomeasure	5		10	10	Reduction	0
	Administrator	3 1 1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Not froated	15
	Administrator	3 1 1	Malware infection	2	Update management (patches) is flawed	The paich are normally done in automatic	2	12	4	4	Nol treated	12
	Administrator	3 1 1	Malware intection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Noi treated	12
	Administrator	a t t	Larging of rights	3	User aufferthostion is not ensured	No password pulcy	1	9	а	a	Not Irealed	в
	Backup	3 1 1	I helt or destruction of media, documents or equipment	8	Backup media are not stored in a suitable plana	The backups are well managed following the good practices	1	0		з	Not Insuled	Ð
	Administrator	3 1 1	Retirenal of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not	6



04. Security Objectives Module

04. Security Objectives Module



- In development
- Facilitates keeping track of the security measures that are implemented and those that still need to be implemented
- Feedback can be given by ILR through platform

NISINP				Incident Natilisation Security Objectives Settings Doplate Rail 🔻 🕫
1 2 3	4 5 6 7 8 9 10	11 12 13 14 15 16 17	18 19 20	0 21 22 25 24 25 26 27 28 25
	ILR_V2: Security roles and responsibilities aintain an appropriate structure of security roles a	id responsibilities.		
Level	Security Measure	Evidence	Measure in place 7	Justification
ILR: Not implemented	No structure of security roles and responsibility.	NA	×	
ILR: Basic	e) Assign security roles and responsibilities to personnel.	i. List of accurity roles (CISO, DPO, business continuity manager, etc.), who occupies them and contact information.		The roles CISO and DPO exist. The name of the persons in charge of these index is officially communicated to any employee.
	b) Make sure the security roles are reachable in case of security incidents.	Reachability rules for security roles (OSO, UPO, business continuity manager, etc.)		The CISO and DEO are reachable 24/7.
ILR: Industry	c) Personnel is formally appointed in security roles.	ii. List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (LISO, DPO), etc.).	×	7
stendard	d) Make personnel aware of the security roles in your organisation and when they should be contacted.	iii. Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.	×	
ILR: State of the art	e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or ped incidents.	 Up to date documentation of the structure of security role assignments and responsibilities. Documentation of review process, taking into account changes and past incidents. 	8	,
		■ 1		

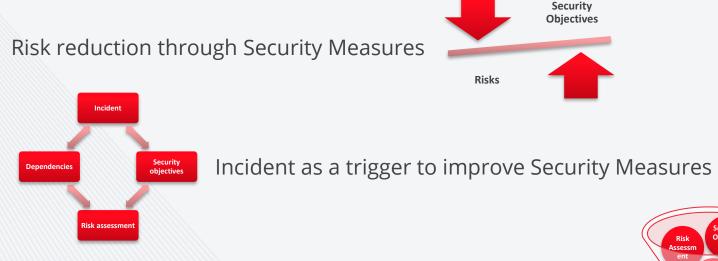


05. Interplay of the Modules

05. Interplay of the modules



Insights through combination of information from different modules



Yearly reports taking into account infos from different modules







Join the SERIMA community!



17, rue du Fossé Adresse postale L-2922 Luxembourg T. : +352 28 228 228 F. : +352 28 228 229 info@ilr.lu

