ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Actions Beyond Words: Automating Audits for Streamlined Cybersecurity Compliance in Europe

23 April 2025

Are you interested in further exploring OSCAL and automated compliance?
We are setting up a Task Force at ECSO!
Reach out to us at policy_team@ecs-org.eu

OSCAL's Role in European Cybersecurity Public Policy

Cristian Tracci

Senior Manager, Policy Analysis and Outreach Stream, ECSO

ECSO

What role does automated compliance play in today's European cybersecurity policy landscape?

How can OSCAL help?

ECSO

EU Policymakers Have Been Very Active

In Brief

Multiple pieces of legislation touching upon cybersecurity were proposed in the last few years and some already entered into force and are being implemented.

Policies intersections and overlaps are growing, making compliance more challenging.

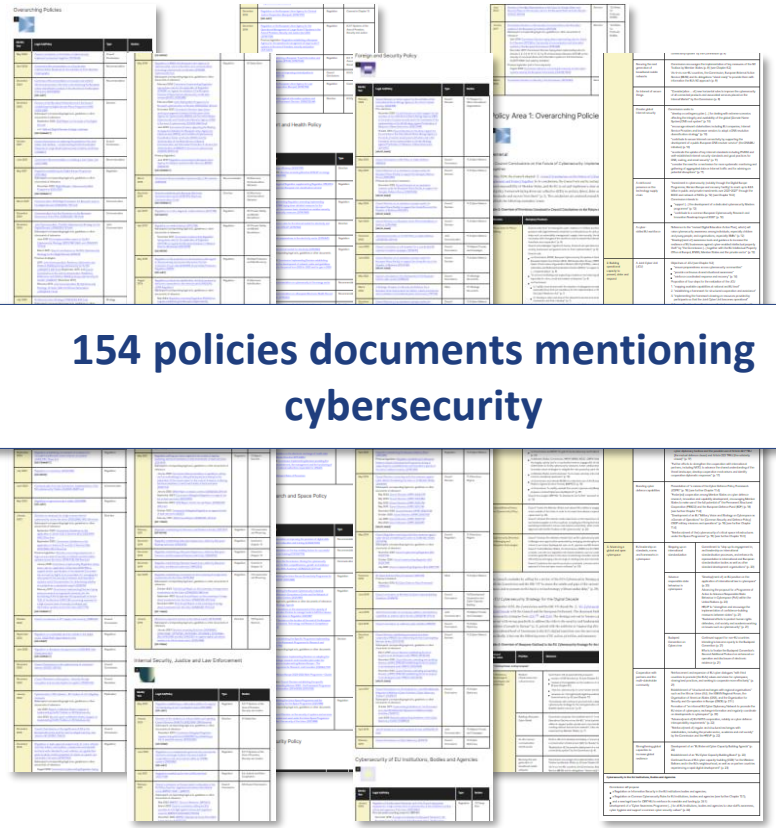
Illustrative list

- NIS2 Directive
- Cyber Resilience Act
- Cyber Solidarity Act
- Cybersecurity Act
- AI Act
- Radio Equipment Directive
- EU Space Law
- Europe's Digital Infrastructure
- 5G Toolbox
- DORA
- EU Digital Identity
- Digital Networks Act

ECSO

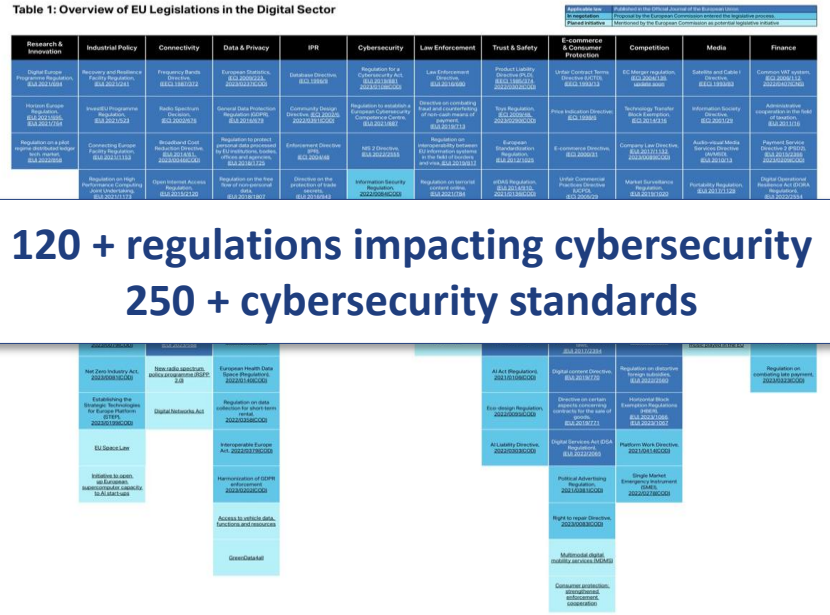
Context

Cybersecurity-related Policies Proliferate



154 policies documents mentioning cybersecurity

Source: Interface



120 + regulations impacting cybersecurity
250 + cybersecurity standards

Source: Bruegel

From Cybersecurity Policies to Audits in Brief

What does it look like concretely?

ECSO

Cybersecurity policies and laws set high-level security domains or requirements

NIS2 Directive

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[…]

Article 21

Cybersecurity risk-management measures

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Cyber Resilience Act (CRA)

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

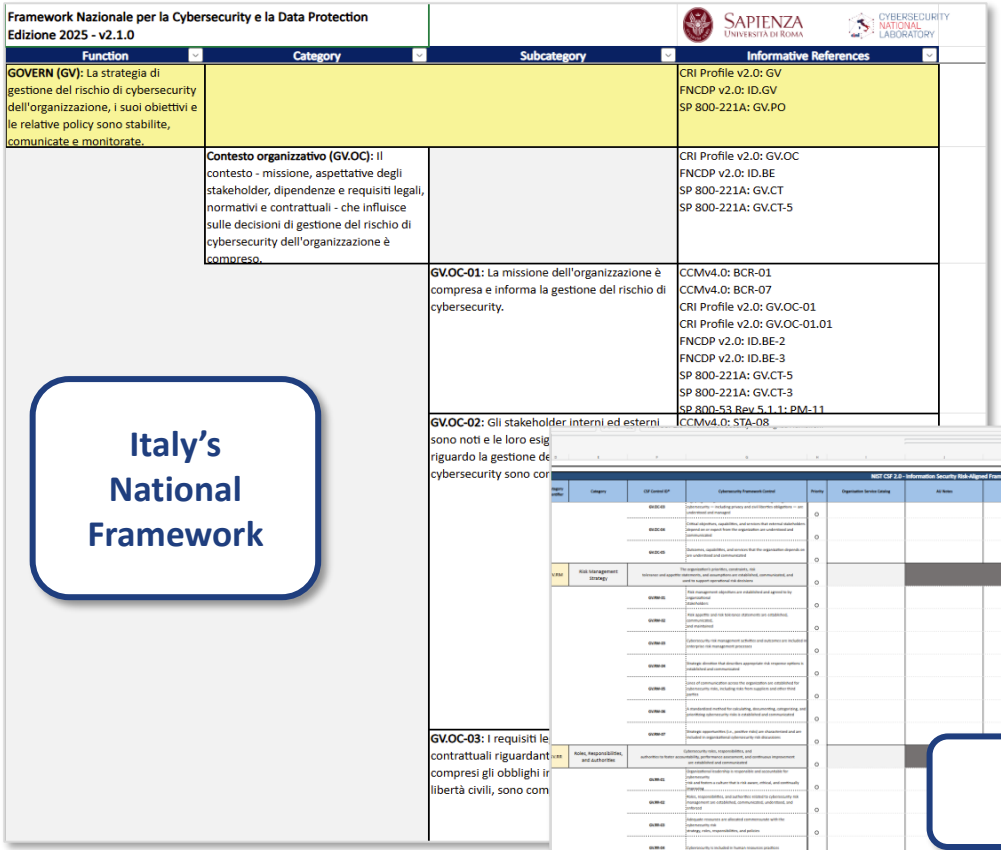
(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and

The security measures are detailed in different security controls frameworks

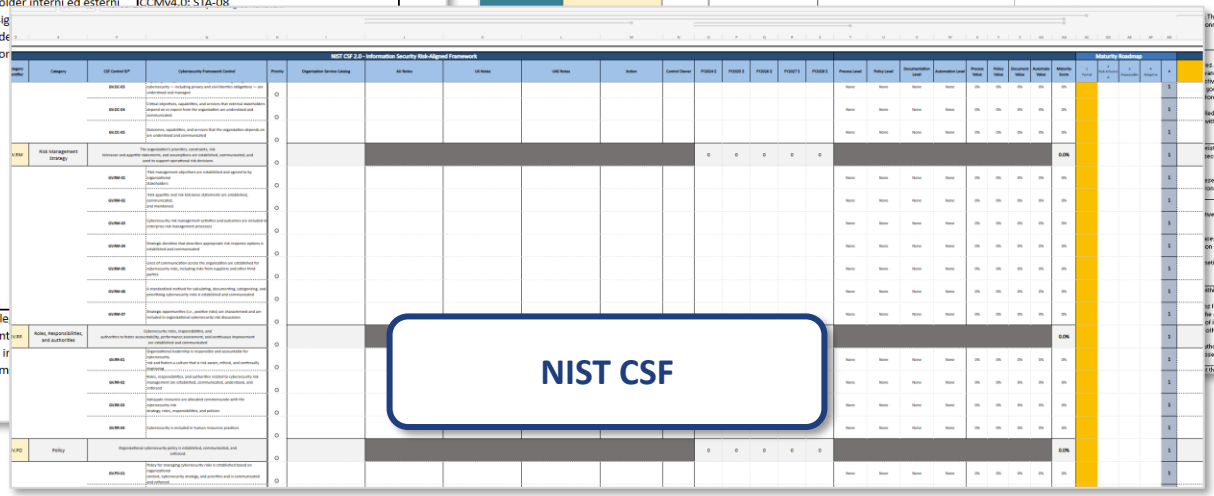
Security controls frameworks rely on assessments via spreadsheet, or


Framework Nazionale per la Cybersecurity e la Data Protection
Edizione 2025 - v2.1.0

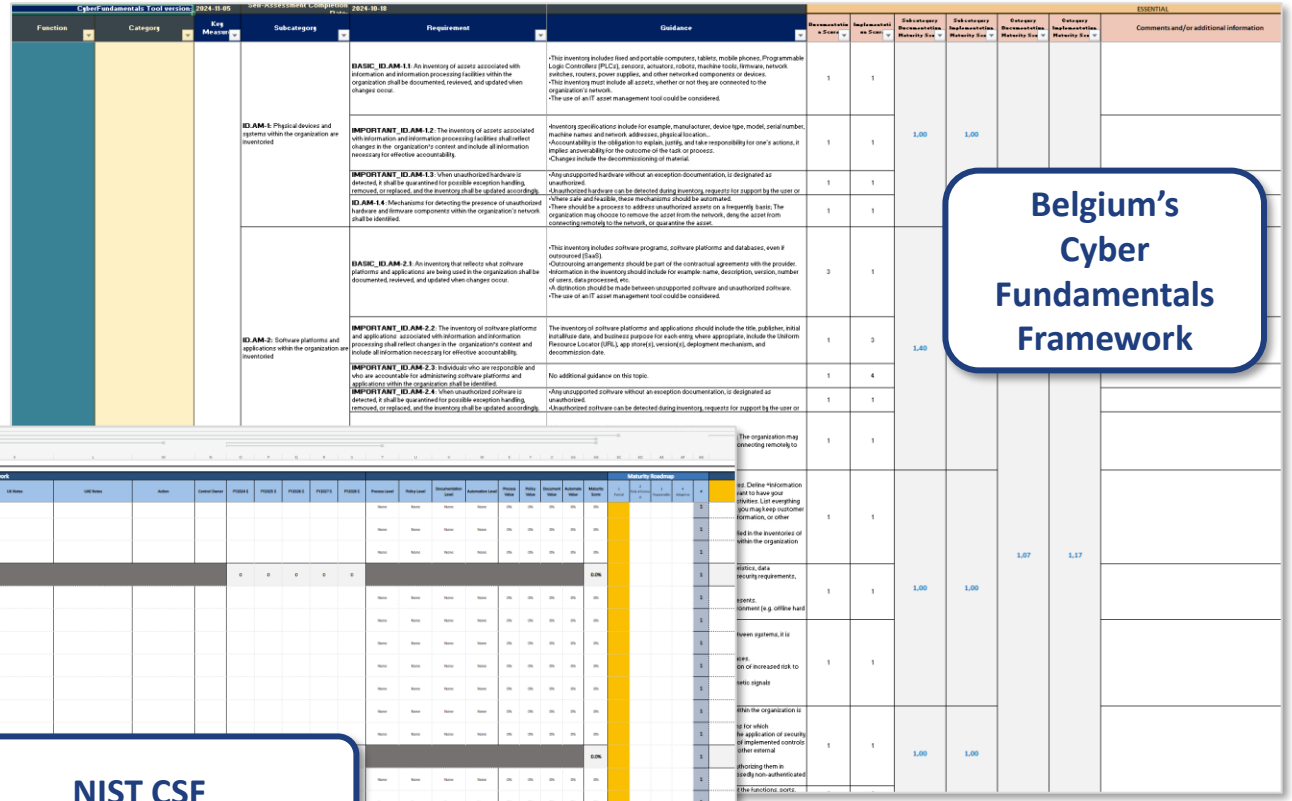
SAPIENZA UNIVERSITÀ DI ROMA — CYBERSECURITY NATIONAL LABORATORY

Function	Category	Subcategory	Informative References
GOVERN (GV): La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate.			CRI Profile v2.0: GV FNCDP v2.0: ID.GV SP 800-221A: GV.PO
	Contesto organizzativo (GV.OC): Il contesto - missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali - che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso.		CRI Profile v2.0: GV.OC FNCDP v2.0: ID.BE SP 800-221A: GV.CT SP 800-221A: GV.CT-5
		GV.OC-01: La missione dell'organizzazione è compresa e informa la gestione del rischio di cybersecurity.	CCMv4.0: BCR-01 CCMv4.0: BCR-07 CRI Profile v2.0: GV.OC-01 CRI Profile v2.0: GV.OC-01.01 FNCDP v2.0: ID.BE-2 FNCDP v2.0: ID.BE-3 SP 800-221A: GV.CT-5 SP 800-221A: GV.CT-3 SP 800-53 Rev 5.1.1: PM-11
		GV.OC-02: Gli stakeholder interni ed esterni sono noti e le loro esig… riguardo la gestione de… cybersecurity sono cor…	CCMv4.0: STA-08
		GV.OC-03: I requisiti le… contrattuali riguardant… compresi gli obblighi ir… libertà civili, sono com…	

Italy's National Framework


NIST CSF 2.0 - Information Security Risk-Aligned Framework

NIST CSF

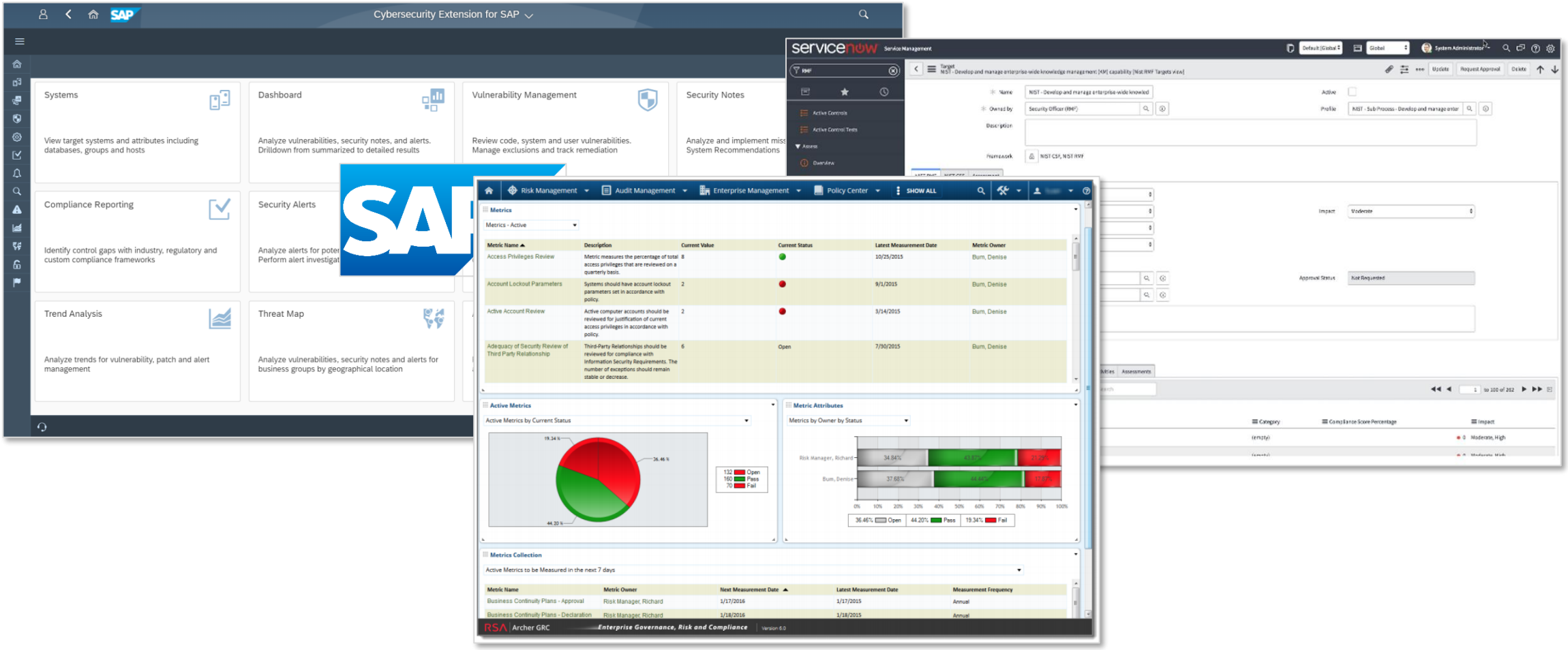

CyberFundamentals Tool version 2024-11-05 — Self-Assessment Completed 2024-10-18

Function	Category	Key Measure	Subcategory	Requirement	Guidance	Documentation Score	Implementation Score	Subcategory Documentation Maturity Sco	Subcategory Implementation Maturity Sco	Category Documentation Maturity Sco	Category Implementation Maturity Sco	Comments and/or additional information
				BASIC_ID.AM-1.1: An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	•This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. •This inventory must include all assets, whether or not they are connected to the organization's network. •The use of an IT asset management tool could be considered.	1	1					
			ID.AM-1: Physical devices and systems within the organization are inventoried	**IMPORTANT_ID.AM-1.2:** The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.	•Inventory specifications include for example, manufacturer, device type, model, serial number, machine names and network addresses, physical location,... •Accountability is the obligation to explain, justify, and take responsibility for one's actions. It implies answerability for the outcome of the task or process. •Changes include the decommissioning of material.	1	1	1,00	1,00			
				IMPORTANT_ID.AM-1.3: When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.	•Any unsupported hardware without an exception documentation, is designated as unauthorized. •Unauthorized hardware can be detected during inventory, requests for support by the user or	1	1					
				ID.AM-1.4: Mechanisms for detecting the presence of unauthorized hardware and firmware components within the organization's network shall be identified.	•Where safe and feasible, these mechanisms should be automated. •There should be a process to address unauthorized assets on a frequently basis; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	1	1					
				BASIC_ID.AM-2.1: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.	•This inventory includes software programs, software platforms and databases, even if outsourced (SaaS). •Outsourcing arrangements should be part of the contractual agreements with the provider. •Information in the inventory should include for example: name, description, version, number of users, data processed, etc. •A distinction should be made between unsupported software and unauthorized software. •The use of an IT asset management tool could be considered.	3	1					
			ID.AM-2: Software platforms and applications within the organization are inventoried	**IMPORTANT_ID.AM-2.2:** The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.	The inventory of software platforms and applications should include the title, publisher, initial installation date, and business purpose for each entry, where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.	1	3	1,40				
				IMPORTANT_ID.AM-2.3: Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be identified.	No additional guidance on this topic.	1	4					
				IMPORTANT_ID.AM-2.4: When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.	•Any unsupported software without an exception documentation, is designated as unauthorized. •Unauthorized software can be detected during inventory, requests for support by the user or	1	1					
						1	1					
						1	1					
						1	1			1,07	1,17	
						1	1	1,00	1,00			
						1	1					
						1	1	1,00	1,00			

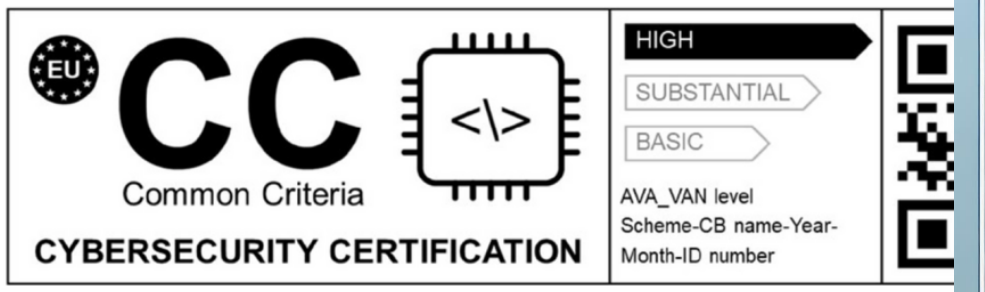
Belgium's Cyber Fundamentals Framework

ECSO

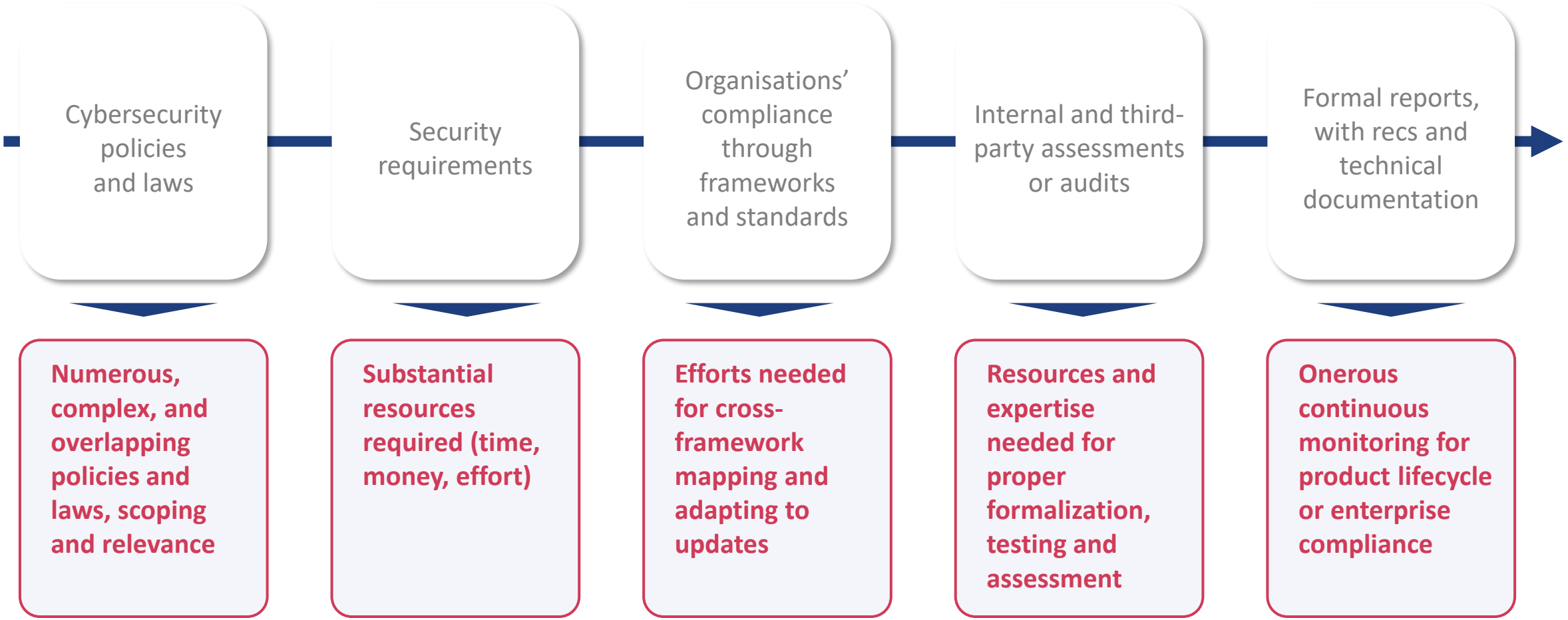
Or GRC tools, supporting the process



Eventually leading to certified audits or product certifications



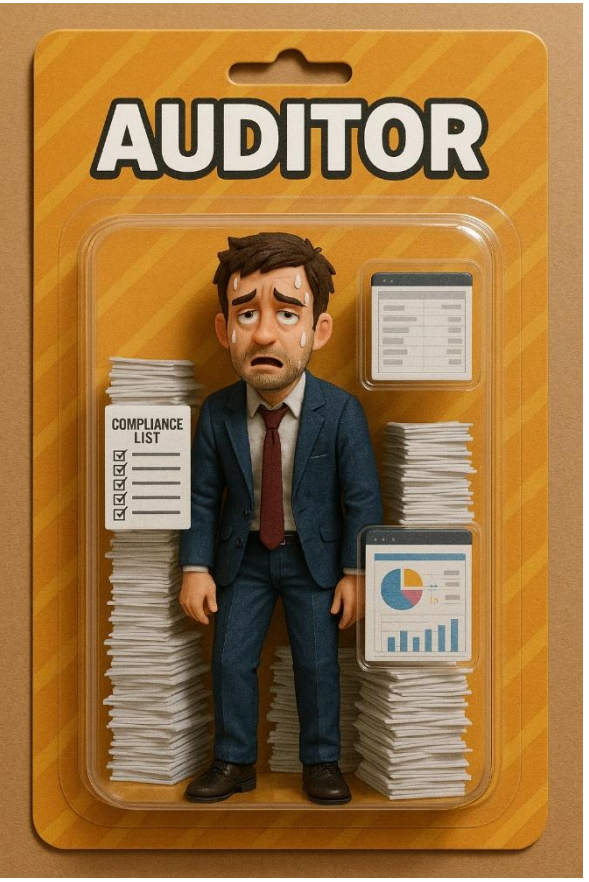
Establishing a Complex Ecosystem



So What?

ECSO

The process remains burdensome: How automated compliance can help



Compliance Challenges In Brief

- Complex procedures
- Resource demands
- Lack of expertise
- Tedious tasks
- Time-consuming processes
- Dependence on external professionals

Europe wants to improve its cybersecurity overall posture

To do so, compliance processes must be improved, to become more efficient and effective.

Automated compliance can assist in achieving this by:

- Providing a standardized approach (common language and processes),
- Facilitating swift assessments, once properly configured,
- Relying on machine-readable formats for sharing and processing audit report,
- Making continuous monitoring a reality, thanks to its automated setup.

Zooming into OSCAL: What's Needed Next?

For discussion

Success Factors	Description	Open Questions
Frameworks	The security controls frameworks, used to comply with the security measures outlined in EU (and global) cybersecurity policies, need to be represented in OSCAL	**Who should do the representation? Should it be done centrally by European and national institutions? Or by independent third parties?**
Tools	OSCAL-based GRC tools need to be developed and brought to market	**Is there an untapped market segment in Europe for OSCAL-based GRC tools?**
Testing	Pilot projects need to be developed and run to test tools and processes and ultimately reach effective and efficient adoption	**Could pilots be run under Digital Europe Program (DEP) projects?**
Adoption	The cybersecurity compliance ecosystem, including both national authorities as well as actors along the supply chain, need to adopt and accept OSCAL reports	**How could national authorities' buy-in be achieved?**

ECSO

What other success factors are there?

What other questions are unanswered?

Are you interested in further exploring how OSCAL and automated compliance?

Reach out to us at policy_team@ecs-org.eu

ECSO