

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 <u>policy_team@ecs-org.eu</u>

OSCAL's Role in European Cybersecurity Public Policy

Cristian Tracci

Senior Manager, Policy Analysis and Outreach Stream, ECSO



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

How can OSCAL help?



Context **EU Policymakers Have Been Very Active**

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

In Brief

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



NIS2 Directive



Cyber Resilience Act



Cyber Solidarity Act



Cybersecurity Act





AI Act



Radio Equipment Directive



Digital Networks Act

EU Digital Identity

EU Space Law

Europe's Digital

Infrastructure

5G Toolbox

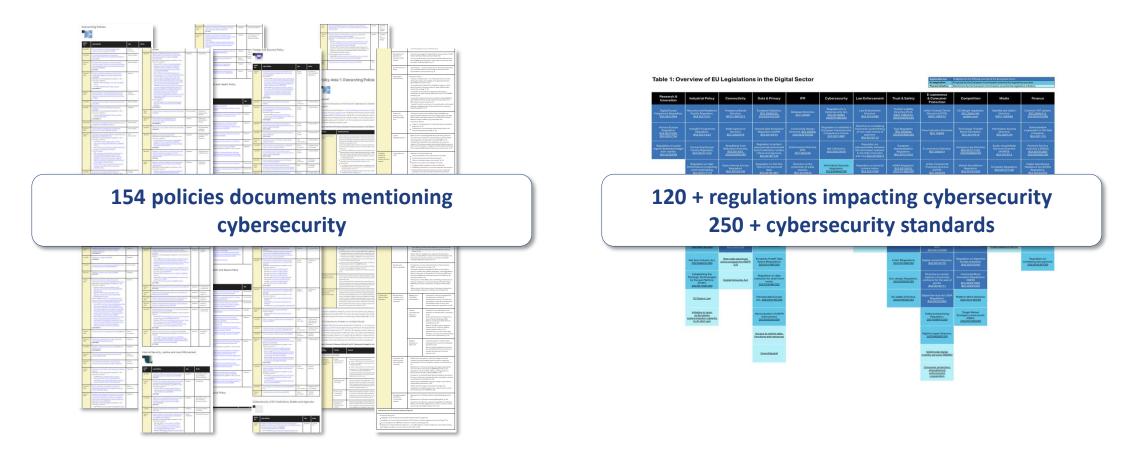
DORA







Context Cybersecurity-related Policies Proliferate



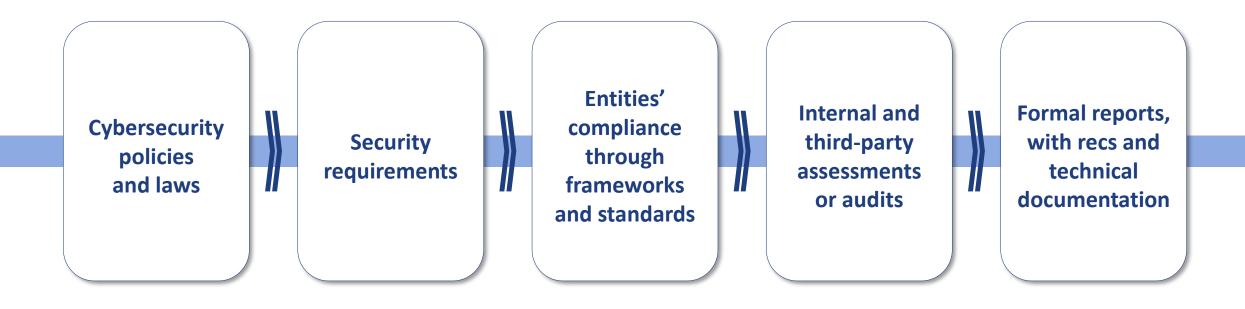
Source: Interface

Source: Bruegel





From Cybersecurity Policies to Audits in Brief







What does it look like concretely?



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

NIS2 Directive

	TNI .
DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	EN 0J L, 20.11.2024
of 14 December 2022	ANNEX I
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	ESSENTIAL CYBERSECURITY REQUIREMENTS
Directive)	Part I Cybersecurity requirements relating to the properties of products with digital elements
[]	 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.
Article 21	to ci of cyberscurry based on the risks.
Cybersecurity risk-management measures	(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
 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 secure: (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. 	 (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 mechanism, 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

Cyber Resilience Act (CRA)



The security measures are detailed in different security controls frameworks





Security controls frameworks rely on assessments via spreadsheet, or

Function V (GV): La strategia di	Category	Subcategory ~	SAPIENZA UNIVERSITÀ DI ROMA Informative Refe CRI Profile v2.0: GV	AATIONAL LABORATORY				DASIC, ID.AM-13: An inventory of assets associated with	This inventory includes fixed and portable computers, tablets, mobile phones, Programm Logic Controllers (PICI2), sensors, actuators, rebork, makine tools, immune, network synthese, routers, poer supplies, and other networked components or devices.			es v Haterity Sc	ny Ostegary tim. Decementation. Im • Materity See • H	nurity Sze 🔻
e del rischio di cybersecurity inizzazione, i suoi obiettivi e			FNCDP v2.0: ID.GV SP 800-221A: GV.PO					information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	panlare, room, poer topper, and an international comparison or events. This inventory must include all access, whether on our they are connected to the organization's network. -The use of an IT asset management tool could be considered.	1	1			
e policy sono stabilite, ate e monitorate.	Contesto organizzativo (GV.OC):		CRI Profile v2.0: GV.OC				ID.AM-E: Physical devices and systems within the organization are inventoried	IMPORTANT_ID.AM-1.2: The inventory of assets associated withinformation and information processing locities 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 num machine names and menorial addresses, physical location. Autocantability is the obligations requires, justing and take responsibility for one's actions implies answerability for the outcome of the task or process. Changes include the decommissioning of material. 	1	1,00	1,00		
	contesto - missione, aspettative degli		FNCDP v2.0: ID.BE					IMPORTANT_ID.AM-1.3: When unauthorized hardware is detected, it shall be guarantined for possible expection handling.	 Any unsupported hardware without an exception documentation, is designated as much mixed. 	1	1			
	stakeholder, dipendenze e requisiti legali, normativi e contrattuali - che influisce		SP 800-221A: GV.CT SP 800-221A: GV.CT-5					removed, or replaced, and the inventory shall be updated accordingly. ID.AM-14 - Mechanizmum for detecting the presence of unauthorize- hardware and immore components vithin the organization's network shall be identified.	-Where safe and feasible, these mechanisms should be automated.	1	1		Be	elgium's
sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso.	cybersecurity dell'organizzazione è								This inversors includes software programs, software platforms and databases, even #					Cyber
	GV.OC-01: La missione dell'organizzazione è compresa e informa la gestione del rischio di cybersecurity.					BASIC_ID.AM-2.1: An inventory that reflects shat software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.	outrourced (SaaS) Outrourced (SaaS) Outrourced an anymeters should be part of the contractual agreements with the provide Information in the inventory should include for example: name, description, version, numb of users, dataprocessed, etc.	н з			-			
						and an	 A distinction should be made between unsupported software and unauthorized software. The use of an IT asset management tool could be considered. 				Fund	damentals		
					ID.AM-2: Software platforms and	and applications, associated with information application	The inventory of software platforms and applications should include the title, publisher, initialituze date, and business purpose for each entry, where appropriate, include the Uniform Resource Locator (URL), and the Uniform and		o		Fra	mework		
		FNCDP v2.0: ID.BE-3				applications within the organization an inventoried	IMPORTANT ID AM-2.3 individuals vito are responsible and	Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.		1,40				
			SP 800-221A: GV.CT-5 SP 800-221A: GV.CT-3					who are accountable for administering software platforms and applications within the organization shall be identified. IMPORTANT_ID_AM-2.4: When unsufficied software is detected it shall be guaramized for costsible exceedion handling.	No additional guidance on this topic. -Any unsupported software without an exception documentation, is designated as unauthorized.	1	4		_	_
		GV.OC-02: Gli stakeholder interni ed esterni	SP 800-53 Rev 5.1.1: PM-11						Unsumorous. -Unsuthorized software can be detected during inventory, requests for support by the user	× '	·			
Italy	'c	sono noti e le loro esig	ICCIVIV4.0, 314-08			·	'		The organization m onnecting remotely t	1	,			
-		riguardo la gestione de	a		с I.		0 F 0 K	s * u v w s *				_		
Natio		sam Gagay Of Control D		Organization Service Lineary All Names	UK Refer	Antes Contribute	nators nations nations 1	19223 Pressiver Relayiers' Concession Advantantum Press	es. Deline *informat	~				
INALIUI	Idi I	active and a second s							Wite Wite Som Print Internet Australia Internet					
		ecces	Other adjustment or appendix on a strainer that external adjustment on a strainer that exte					Nere Nore Nore Of OS	m m m 1 stvites. List everythi sou maj keep outo	ng mer 1				
Framew		active and a second s	Anima and a second and a s					Nore Nore Nore Nore Oil Nore Nore Nore Nore Oil Nore Nore Nore Nore Oil	m m m 1 bittine. Lite everythic been putto to formation, or other methods and the investorie with the investorie with the expansion.	ng mer 1	1			
		0.000 0.000 0.000 0.000	Intervention Andream				0 0 0 0	Bars Bars <th< td=""><td>m m<td>ng mer 1</td><td>1</td><td></td><td>1,07</td><td>1,17</td></td></th<>	m m <td>ng mer 1</td> <td>1</td> <td></td> <td>1,07</td> <td>1,17</td>	ng mer 1	1		1,07	1,17
			Datases, spallite, and ansars for the signature dependent or understand annunced O	_			• • • •	Bars Bars <th< td=""><td>a a b</td><td>199 190 1</td><td>1 1.00</td><td>1,00</td><td></td><td>1,17</td></th<>	a a b	199 190 1	1 1.00	1,00		1,17
		AN	Datases, spalities, and ansars that the against an algorithm datases of the transmission of the second seco	-			• • • •	No. No. <td>m m m m m m m m m m m m m m m m m m m</td> <td>199 190 1</td> <td></td> <td>1,00</td> <td></td> <td>1.17</td>	m m m m m m m m m m m m m m m m m m m	199 190 1		1,00		1.17
		ADD ADD ADD VM Mit Stargerst ADD VM Mit Stargerst ADD	Datases, spalities, and ansars that the against an algorithm datases of the transmission of the second seco	-				No. No. <td>a a b</td> <td>199 190 1</td> <td></td> <td>1,00</td> <td></td> <td>3.17</td>	a a b	199 190 1		1,00		3.17
		ADD ADD ADD	immund 0 therease any advectory of the system of the syst					No. No. <td>n n</td> <td>n g g g g g g g g g g g g g g g g g g g</td> <td></td> <td>1.00</td> <td></td> <td>1.17</td>	n n	n g g g g g g g g g g g g g g g g g g g		1.00		1.17
		m m m m m m m m m m m Max agent m m m m Max agent m m m m Max agent m m m	immund 0 therease any advectory of the system of the syst					No. No. <td>n n</td> <td>n g g g g g g g g g g g g g g g g g g g</td> <td>1, 1.00</td> <td>1.00</td> <td></td> <td>ι.υ </td>	n n	n g g g g g g g g g g g g g g g g g g g	1, 1.00	1.00		ι.υ
		Image: Section 1 Image: Section 2 Image: Section 2<	ammania 0 Ammania				• • • •	N N N N N N N I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I	Image: Constraint of the	n g g g g g g g g g g g g g g g g g g g	1, 1.00	1.00		£.17
			Initial Control of the second					N N N N N N N I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I	Image: Constraint of the	n n n n n n n n n n n n n n n n n n n	1	1.00		£.17
		MB LA ADA 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400 400	Image: Section 1 Image: Section 1<					N N N N N N N I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I	Image: Constraint of the	n n n n n n n n n n n n n n n n n n n	1, 1.00			£.17
		GVOC-03: I requisit le contrattuali riguardant te distance de contrattuali riguardant te distanc						N N N N N N N I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I	Image: Constraint of the	n n n n n n n n n n n n n n n n n n n	1			L17
		GV.OC-03: I requisit le comprese i de holie hier GMOC-03: I requisit le comprese i de holie hier comprese i de holie hier		ſ	NIS	ST CSF		N N	Image: Constraint of the	n n n n n n n n n n n n n n n n n n n	1			L37
		GVOC-03: I requisit le contrattuali riguardant un dinatori di anti- contrattuali riguardant un di anti- contrattuali riguardan	Image: Section of the sectio	ſ	NIS	ST CSF	• • • •	N N	Image: Constraint of the		1			£.17
		GV.OC-03: I requisit le contrattual riguardant ta information de la contrattual de la contrattual riguardant ta information de la contrattual riguardant t			NIS	ST CSF		N N	Image: Constraint of the		1			L17
		GV.OC-03: I requisit le more compresi gli obblighi ir libertà civil, sono com	Image: Section of the sectio	(NIS	ST CSF		N N	n n		1			L17

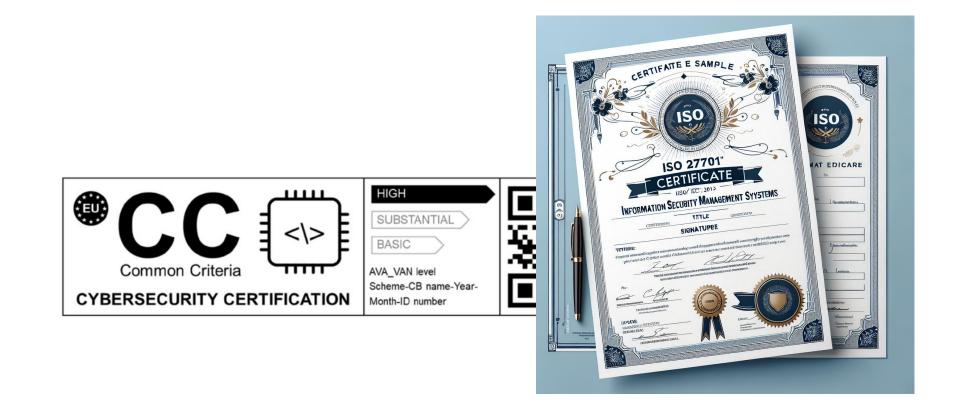


Or GRC tools, supporting the process

	2 < a 💁	Cybersecurity Exter	nsion for SAP \checkmark		Q					
					servicenov	Service Nanagement			Default (Giobal # E	🛙 Giobal 🕴 🌐 System Administrates) - 🔍 🗗 🛞 🎯
					(7 He				-	P Ξ *** Updata Request Approval Delete ↑ ↓
								knowledge management (KM) capability (Mot RMF Targets view)		
ą <mark>ي</mark>	Systems	Dashboard	Vulnerability Management	Security Notes	□ ★	<u> </u>		Develop and manage enterprise-wide knowled	Active	
6		-0	~		Active Controls			rity Officer (1947)	Profile	If - Sub Process - Develop and manage enter 0, 0
	View target systems and attributes including	Analyze vulnerabilities, security notes, and alerts.	Review code, system and user vulnerabilities.	Analyze and implement mis	Active Control Tests		Description			
Ľ	databases, groups and hosts	Drilldown from summarized to detailed results	Manage exclusions and track remediation	System Recommendations	▼ A029		Fremework 🙆 1	NST CSF, NST RVF		
					() Detrára	LIPPOLE MARKAR				
			🟫 🗇 Risk Management 👻 🗐 Audit Managemen	👻 📕 Enterprise Manageme	ent 👻 📃 Policy Center	- SHOW ALL	۹ 🛠 - ۲	· · · · · · · · · · · · · · · · · · ·		
▲	Compliance Reporting	Security Alerts							Impact Vo	Sector 0
1			Metrics - Active					•		
5€	Identify control gaps with industry, regulatory and	Analyze alerts for poter	Metric Name Description		Current Status	Latest Measurement Date	Metric Owner	• • • •		
	custom compliance frameworks	Perform alert investigat	Access Privileges Review Metric measures the percentage of tot access privileges that are reviewed on quarterity basis.		•	10/25/2015	Bum, Denise	1		
•			Account Lockout Parameters Systems should have account lockout parameters set in accordance with	2	•	9/1/2015	Bum, Denise	Q (0)	Approval Status Ko	Requested
	The second secon	Thursday 14	policy. Active Account Review Active computer accounts should be	2		3/14/2015	Bum, Denise	G (0		
	Trend Analysis	Threat Map	reviewed for justification of current access privileges in accordance with			472472025	burn, benae			
			policy. Adequacy of Security Review of Third-Party Relationships should be	6 0	Open	7/30/2015	Burn, Denise			
	Analyze trends for vulnerability, patch and alert	Analyze vulnerabilities, security notes and alerts for	Third Party Relationship reviewed for compliance with Information Security Requirements. Th							
	management	business groups by geographical location	: number of exceptions should remain stable or decrease.					Atties Assessments		
			Active Metrics		Metric Attributes					44 4 1 to 100 of 252 > >> E
			Active Metrics by Current Status		Metrics by Owner by Status					icore Percentage Impact
	Q		19.34 8		1				(ensty)	0 Moderate, High
			-36.46 %		Risk Manager, Richard –	34.84%	13.87% 21.2		lameted	· A Madazata Mide
				132 Open 160 Pass 70 Fail	Bum Denixe=	37.68%	11.112			
				70 Fail	buil, belise	31.00%				
						10% 20% 30% 40% 50%		2% 10.0%		
			44.20 %		36.46%	Open 44.20% Pass 1	19.34% Fail			
			A Cill Maniar Collection	(ە	(h					
			Active Metrics to be Measured in the next 7 days							
			Metric Name Metric Owner	Next Measurement Date	Latest Measure	ment Date Measu	urement Frequency			
			Business Continuity Plans - Approval Risk Manager, Richard	1/17/2016	1/17/2015	Annua				
			Business Continuity Plans - Declaration Risk Manager, Richard	1/18/2016 Risk and Compliance Version 6	1/18/2015	Annua	al			

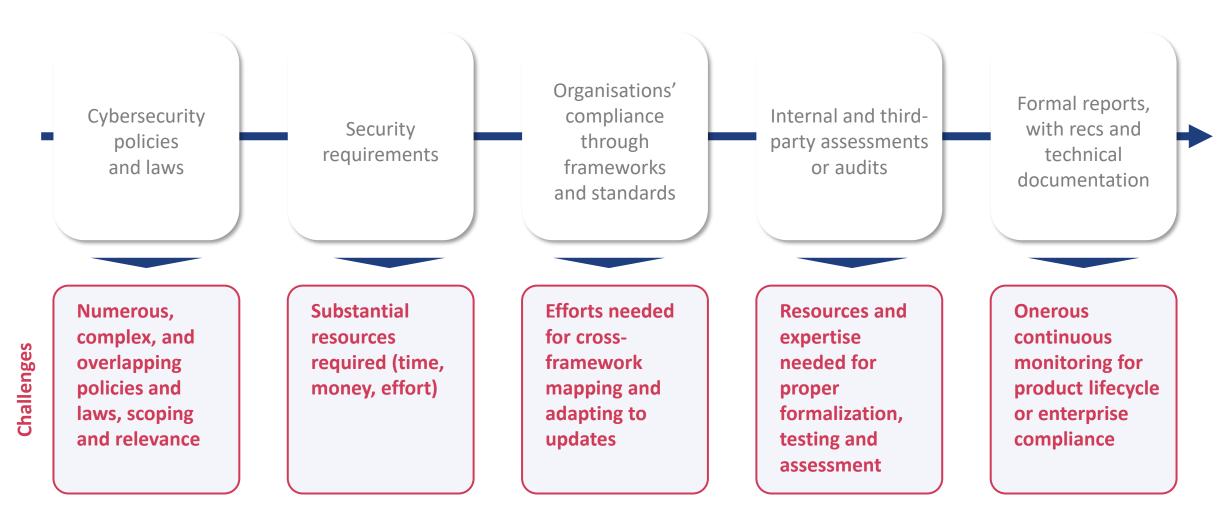


Eventually leading to certified audits or product certifications





Establishing a Complex Ecosystem







So What?



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?

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?					





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

