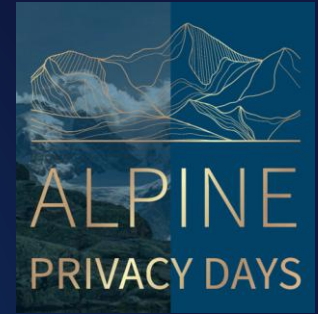


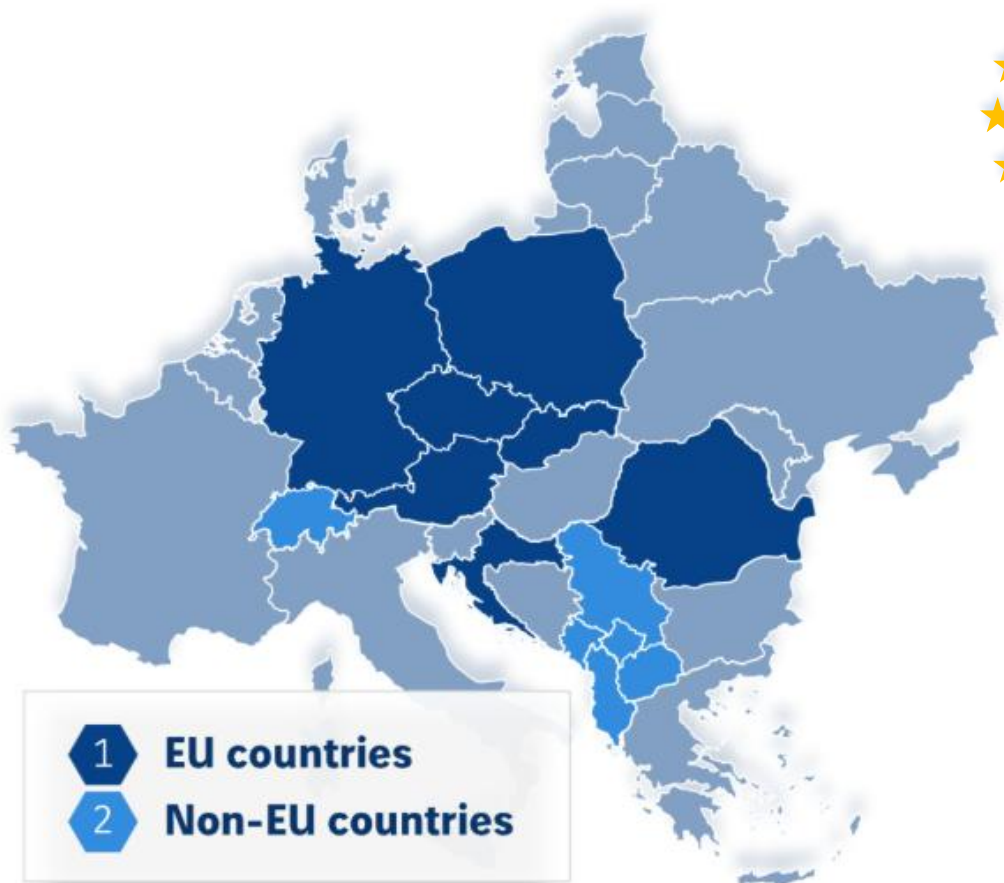


NIS2 & DORA Workshop



Many countries But one challenge

How to create one common
Standard if every country can
implement NIS2 in their own
way?





NIS 2: Directive Meets Regulation

NIS 2 must be understood from two legal perspectives: the overarching Directive and the directly applicable Regulation. Together, they shape both the strategic goals and the precise technical rules for EU-wide cybersecurity.

Aspect	NIS2 Directive (EU) 2022/2555	NIS2 Implementing Regulation (EU) 2024/2690
Role	Sets objectives & obligations for Member States	Provides technical & methodological detail for specific NIS 2 provisions
Legal Nature	Directive – requires national transposition	Regulation – directly applicable, no transposition
Flexibility	Wording and approach can vary nationally (within EU goals)	Uniform rules across all Member States
Scope	Sectors covered, governance, general requirements	Risk-management measures, criteria for “significant incident”
Example	Obligation to report significant incidents	€500 000 threshold for financial impact in incident definition
Link	Directive (EU) 2022/2555	Regulation (EU) 2024/2690



ENISA GUIDANCE

TECHNICAL IMPLEMENTATION GUIDANCE

- Draft published in October 2024, Final in late June 2025
- Supports this implementing regulation by providing:
 - guidance, that is, indicative and actionable advice on parameters to consider when implementing a requirement;
 - examples of evidence, that is, the types of evidence that a requirement is in place; and
 - mappings from security requirements to industry good practices, European and international standards, and national frameworks.
- Provides comprehensive coverage of the technical and methodological requirements mandated by the NIS2, offering practical advice, best practices, and mapped evidence examples for 13 core cybersecurity domains.





Mapping of NIS2 to ISO 27.001

Remaining Gaps to Address

≈90%
Compliance

An organization certified under ISO/IEC 27001:2022 is typically around 90% compliant with the NIS2 Directive, provided the ISMS is properly implemented.*

What is the 10% Gap?

Key NIS2 Obligation	ISO 27001 Coverage	NIS2 Article	Summary
Executive liability and governance	✗ Not covered	Article 20	NIS2 makes top management legally accountable for cybersecurity. They must oversee and approve cyber measures and receive regular training.
Mandatory incident reporting to authorities	✗ Not covered	Article 23	Must notify national CSIRT or regulator of major incidents within 24h (early warning) and 72h (detailed report).
Cooperation with national authorities	✗ Not covered	Articles 23–28	Entities must cooperate with audits, inspections, and follow binding instructions from authorities.
Use of EU-certified cybersecurity technologies	✗ Not covered	Article 24	May be required to use EU-certified ICT products/services under EU cybersecurity certification schemes.
Enforcement & penalties for non-compliance	✗ Not covered	Article 34	Failure to comply may result in fines up to €10M or 2% of global revenue for essential entities.
Supply chain cybersecurity oversight	⚠ Partially covered		Entities must assess and manage supply chain security risks, including third-party vulnerabilities and development practices. ISO covers this broadly.

*Mandatory: The report from the most recent ISO 27001 certification must be provided.



INTERNAL NIS2 COMPLIANCE INITIATIVE



PROJECT PHASES

Phase	1	Affectedness Analysis	2	Training & Awareness	3	Gap Analysis	4	Remediation & Implementation	5	Approval
Objective	Identify legal entities and BUs affected by NIS2		Educate BUs on obligations & process		Assess compliance using NIS2 Audit Kit		Close gaps to reach compliance		Formally confirm and certify compliance	
Key Activities	Identify affected legal entities		- Create NIS2 Audit-Kit - Prepare and deliver training		Distribute Audit Kit CISO evaluates submissions and identifies gaps		BUs implement action items CISO advises on solutions		Final compliance review Collect signed declarations	
Deliverables	Excel overview with Legal Entities		- Training materials - NIS2 Audit-Kit		Gap reports based on Audit Kits		Action plans Implementation evidence Status dashboard		Signed NIS2 Compliance Acknowledgment Form	
Responsibilities – Legal/CISO	Provide the list of all legal entities and do the Affectedness Analysis		- Develop training, conduct sessions - Provide Q&A support		- Analyse submissions - Support NIS2 responsible person per Legal Entity		- Advice on implementation - Track status		- Perform review - Issue internal Approval	
Responsibilities – Legal Entity	No Todo		- Confirm understanding of obligations - Name NIS2 responsible FTE		- Complete Audit Kit (Self-Assessment) - Deliver documentation		- Execute action items - Implement controls		- Sign declaration - Confirm compliance	
Planned Duration	June 2025		July-September 2025		September, October 2025		November 2025		December 2025	

Current phase



Phase 1

Affectedness Analysis

In this phase, the Legal Department **determines which Legal Entities fall under the scope of the NIS2 Directive**, guided by the directive itself and the supporting technical implementation rules outlined in Commission Regulation (EU) 2024/2690 ([EUR-Lex reference](#)). All Legal Entities that offer services as Digital Infrastructure or Online Service Providers, as defined under Article 2(2) of the regulation, are considered in scope under NIS2.

To ensure consistency and avoid fragmented compliance:

- ▶ If a **Legal Entity includes multiple Business Units (BUs)** and only one BU is in scope, **then all BUs within that Legal Entity must comply with NIS2.**
- ▶ An Excel-based overview is created to document affected Legal Entities and their corresponding BUs.





Phase 2: Training & Awareness Skillset for NIS2 Responsible Person

To ensure NIS2 compliance, **Managing Directors need to appoint a NIS2 Responsible Person** who leads and coordinates the implementation of requirements across Business Units. **This person must have a clear mandate to engage with all units directly and enforce necessary measures.**

This person should have the following skills:

- Experienced with risk management and security frameworks (e.g., ISO 27001, NIST)
- Familiar with IT infrastructure, network security, and vulnerabilities
- Capable of leading implementation projects across Bus
- Knowledge of or willingness to learn about data protection (GDPR)

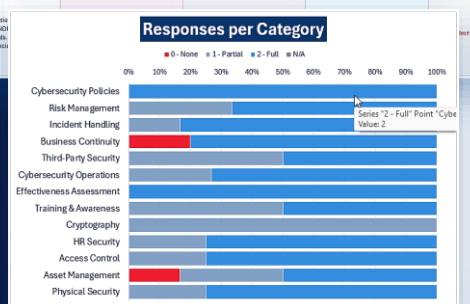


OVERVIEW

- Designed as a part of VINCI Energies' commitment to comply with the NIS2.
- Designed to simply **self-assessment**, conduct **internal and external audits**.
- Based on **ENISA Guidance** and covers all 13 domains.
- Contains:
 - High-level and in-depth questions for assessing cybersecurity posture and NIS2 compliance.
 - Response options with examples of evidences.
 - Scope setup for varios scenarios and respondents.
 - Scoring page with visualization graphs.
 - References and glossary.



Assessment				TEAM				
Meta Data				Levels				
#	Level of Responsibility	Category			2 - Full	Response		
101001	1 - Global CISO (Y)	1. Policy On the Security Of Network And Information Systems	Does your organisational Security Policy and information sign		Not is incomplete to govern approval, or created and not prepared.	Acceptance policy, covering all network and information systems, rules, responsibilities, and that it is responsible for being documented, approved by senior management, and actively communicated to all interested persons, who confirm understanding.	2 - Full	
101002	1 - Global CISO (Y)	1. Policy On the Security Of Network And Information Systems	Is the CISO regularly reviewed and updated to reflect current cyber security risks and regulatory requirements.	Policy approval date (e.g., formal management body sign-off/recorded research, and information security policy) is less than year ago.	The policy has not been reviewed since issuance for was last reviewed more than two years ago and does not incorporate recent threat trends or regulatory changes.	The policy is reviewed, but reviews are irregular (e.g., ad hoc or exceeding 12 months without trigger) or updates address only some risk/regulatory, evidence of formal approval or tracked changes is incomplete.	The policy is reviewed on a defined schedule and annually and promptly after significant events or regulatory updates, reviews are documented, formally approved, and communicated to all relevant stakeholders.	2 - Full
101003	1 - Global CISO (Y)	1. Policy On the Security Of Network And Information Systems	Are roles, responsibilities, and authorities related to network and information security clearly defined and documented?	- Organisational charts showing cybersecurity roles and responsibilities. - Job descriptions specifying cybersecurity duties and authorities. - Security role documentation (e.g., current structure of security roles).	Roles, responsibilities, and authorities are not documented, staff are unclear who is accountable for security activities.	Some roles are described, but coverage is incomplete, outdated, or not communicated, leaving overlaps or gaps in accountability.	All security related roles, responsibilities, and authorities are clearly defined, documented, reviewed, updated, and communicated, every body has a clearly assigned owner.	2 - Full





Phase 5

Confirmation of NIS2 Compliance

At the end of Phase 5, each Managing Director must sign a formal declaration confirming that all NIS2 controls have been properly implemented within their area of responsibility.

This signed confirmation:



- ▶ Serves as formal proof of compliance



- ▶ Is required for issuing the internal NIS2 Compliance Certificate



- ▶ Marks the successful completion of the compliance process for the Business Unit

VINCI

NIS2 Compliance Acknowledgment Form



Legal Entity: _____

Name Managing Director: _____

Date: _____

Signature: _____

Recitals

WHEREAS Directive (EU) 2022/2555 (the NIS2 Directive) establishes binding cybersecurity requirements that apply directly to legal entities as defined under applicable national and European legislation,

WHEREAS the NIS2 Directive explicitly does not recognize internal organizational structures, such as the Business Unit logic used within VINCI Energies, for the purpose of regulatory compliance,

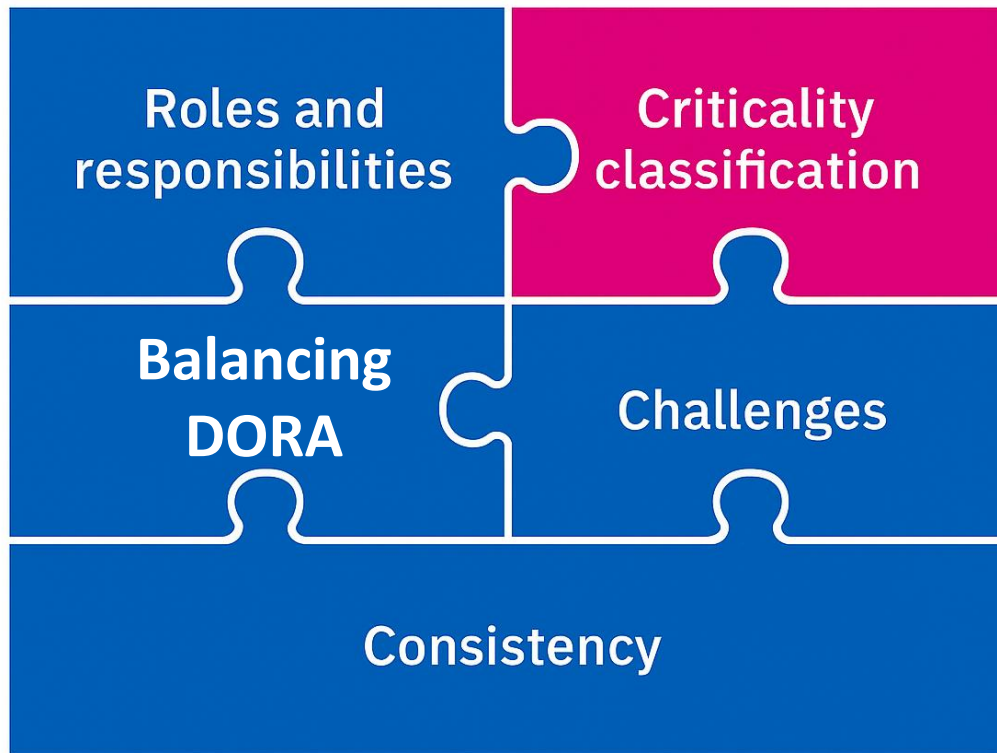
WHEREAS each legal entity bears independent responsibility for fulfilling NIS2 obligations, and its management may be held personally accountable in the event of non-compliance,

NOW, THEREFORE, the undersigned acknowledges and agrees as follows:

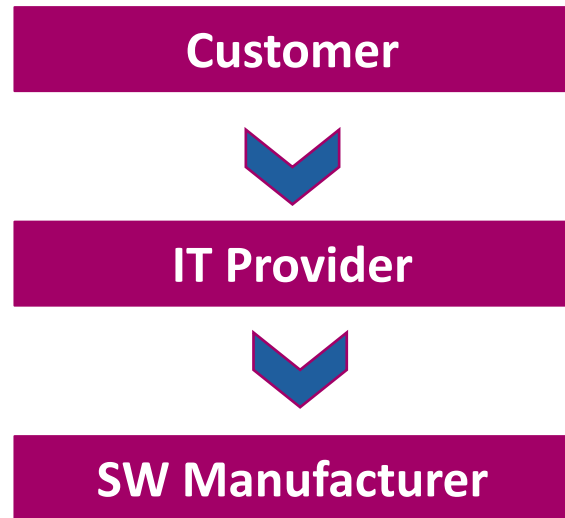
Version 1.0 | Révisé le 04/09/2024 | Copyright VINCI Energies Schenker AG | Page 1 sur 1



Piecing Together Regulatory Clarity



A Tricky Piece in the DORA Puzzle



A dramatic coastal scene featuring a lighthouse and a stone sea wall during a storm. The lighthouse is a tall, cylindrical structure with a white lantern room, situated on a rocky outcrop. A stone sea wall, built from large, rectangular blocks, runs along the coast, with waves crashing over it and creating a series of cascades. The sky is a deep, dark blue, and the water is a turbulent, dark blue-grey. The overall mood is one of power and resilience.

axians

Thank you!