



Cybersecurity Checkmate:

DORA/NIS2 and YOU

Dr. Leila Taghizadeh

Global Head of Cyber Risk Management
& CISO @Allianz

<https://www.linkedin.com/in/leilataghizadeh/>

Agenda

- **Introduction: DORA & NIS2**
- **How to become NIS2 Compliant**
- **How to become DORA Compliant**





DORA & NIS2

DORA is a binding regulation applicable to the financial sector.

NIS2 is a directive that sets cybersecurity goals for EU countries, allowing flexibilities in implementation.

Both play crucial roles in enhancing digital resilience and security across Europe.

DORA and Supplementary Documents

- **Chapter I: General Provisions:** Contains foundational provisions applicable throughout DORA. Includes definitions, scope, and the proportionality principle.
- **Chapter II: ICT Risk Management:** Divided into sections addressing governance, organization, and risk management. Specifies requirements related to ICT risk management.
- **Chapter III: Incident Reporting and Management:** Focuses on reporting major ICT incidents, defines timelines, templates, and criteria for classification.
- **Chapter IV: ICT Third-Party Risk Management:** Addresses governance arrangements, risk management, and internal controls related to third-party service providers.
- **Chapter V: Final Provisions:** Covers miscellaneous matters, including the entry into force of DORA.
- **RTS* on ICT Risk Management Framework** provides guidelines for harmonizing ICT risk management.
- **RTS on Incident Classification Criteria** specifies how to classify major ICT incidents.
- **RTS on ICT Third-Party Policy (TPP)** governs third-party risk management.
- **ITS** on the Register of Information** to establish the templates for the register of information.

Public Authorities for DORA

The ESAs published

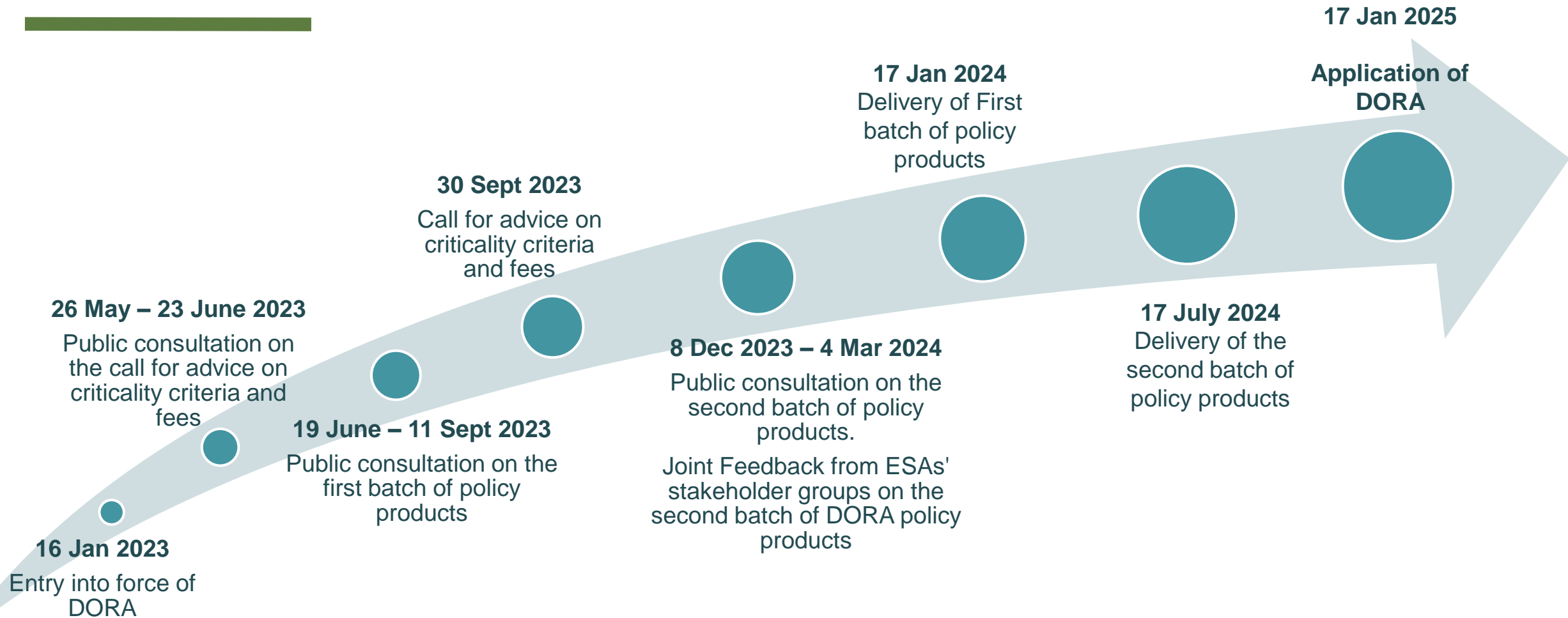
- Digital Operational Resilience Act (DORA)
- Three regulatory technical standards (RTS),
- One Implementing Technical Standards (ITS)

aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks.

The ESAs are the three European Supervisory Authorities

- **EBA (European Banking Authority):** Primarily oversees the banking sector.
 - Develops single rulebooks for EU banks.
 - Conducts stress tests and risk assessments.
 - Promotes supervisory convergence and ensures consistent application of EU banking rules.
- **EIOPA (European Insurance and Occupational Pensions Authority):** Regulates insurance and occupational pensions.
 - Develops common EU insurance and pension rules.
 - Conducts risk assessments.
 - Promotes supervisory convergence and ensures consumer protection.
- **ESMA (European Securities and Markets Authority):** Regulates securities markets and financial instruments.
 - Develops common EU securities rules.
 - Supervises credit rating agencies and trade repositories.
 - Ensures market integrity and investor protection and promotes supervisory convergence.

Journey of DORA

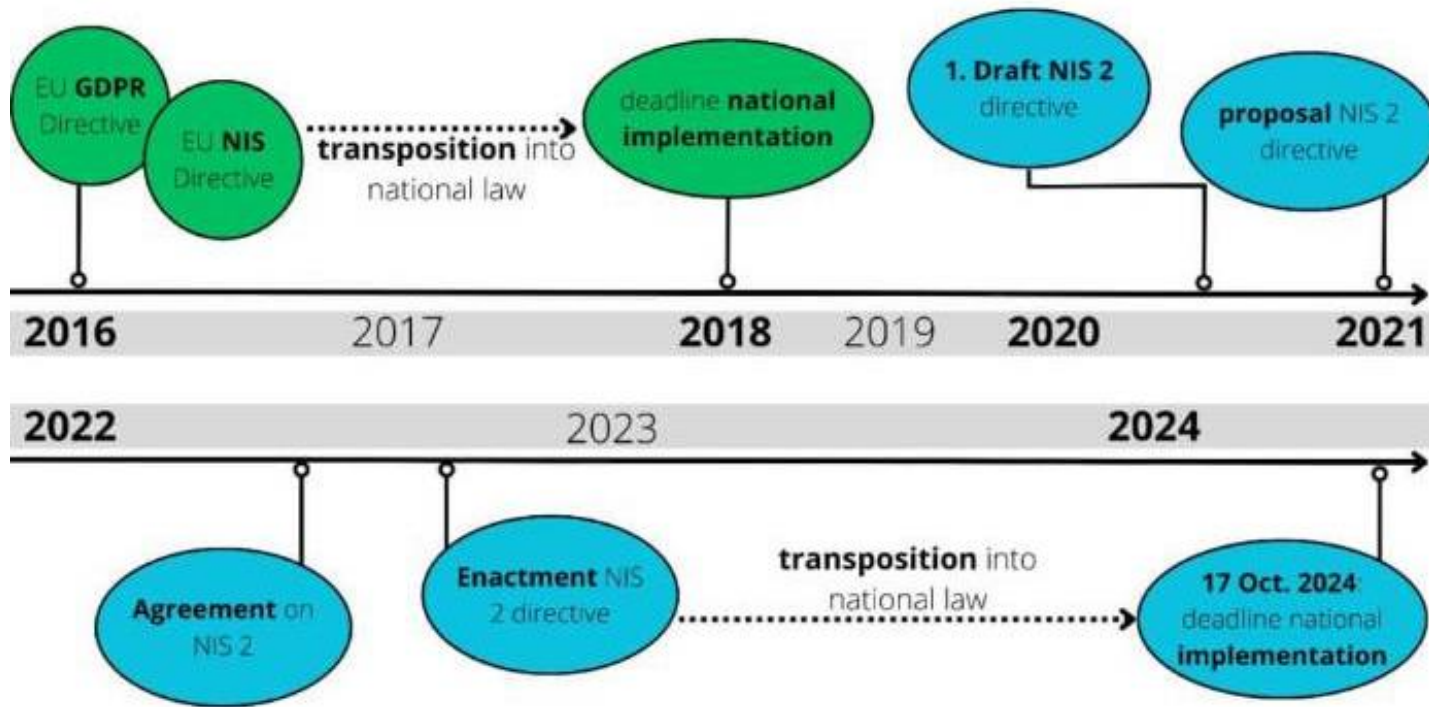




Objective: The primary goal of the NIS2 Directive is to achieve a high common level of cybersecurity across the European Union (EU) Member States. It recognizes the growing threats posed by digitalization and the surge in cyber-attacks.

Background: Prior to NIS2, the original NIS Directive was the first EU-wide legislation specifically addressing cybersecurity. However, its implementation faced challenges, resulting in fragmentation across the internal market.

Network and Information Security (NIS2) Directive



NIS Timeline

- **Scope Expansion:** NIS2 effectively obliges more entities and sectors to take cybersecurity measures, contributing to increased resilience in Europe in the long term.
- **Stricter Oversight from the EU:** NIS2 introduces more stringent supervisory measures and harmonized sanctions across the EU.
- **Streamlined Reporting and Information Sharing Obligations:** NIS2 introduces new reporting and information sharing mechanisms for efficient incident response.



NIS2 builds on 3 main pillars of NIS Directive

NIS-2 Scope – Final version

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees or more than 50 million revenue)	Medium (more than 50 employees or more than 10million revenue)	Small & Micro	
Annex I: Sectors of high criticality							
1. Energy	Electricity; district Heating & cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society	
2. Transport	Air; Water; Rail; Road						
	Special case: Public Transport: only if identified as CER						
3. Banking	Credit institutions (attention: DORA lex specialis)						
4. Financial Market Infrastructure	Trading venues, central counterparties (attention: DORA lex specialis)						
5. Health	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency						
	Special case: entities holding a distribution authorization for medicinal products: only if identified as CER						
6. Drinking Water		Essential	Essential	Essential	Essential	Essential	
7. Waste Water	(only if it is an essential part of their general activity)						
8. Digital Infrastructure	Qualified trust service providers						
	DNS service providers (excluding root name servers)						One stop: Only the MS where they have their main establishment
	TLD name registries						Member State in which they provide their services
	Providers of public electronic communications networks						The Member State(s) where it is established
	Non-qualified trust service providers						Essential
	Internet Exchange Point providers						
	Cloud computing service providers						
	Data centre service providers						
	Content delivery network providers	One stop: Only the MS where they have their main establishment					
8a. ICT-service management	Managed (Security) Service Providers	MS that established them	Essential	Essential	Essential	Essential	
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks, defence, national or public security); Of regional governments: risk based. (Optional for Member States: of local governments)						
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important	
Annex II: other critical sectors							
1. Postal and courier services		The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society	
2. Waste Management	(only if principal economic activity)						
3. Chemicals	Manufacture, production, distribution						
4. Food	Production, processing and distribution						
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)						
6. Digital providers	online marketplaces, search engines, social networking	One stop: Only the MS where they have Main establishment					
7. Research	Research organisations (excluding education institutions)	Member State(s) where established					
Entities providing domain name registration services		One stop: Only the MS where they have Main establishment	All sizes, but only subject to Article 3(3) and Article 29				



The Scope: NIS1 & NIS2

The Scope: NIS2



Essential | Proactive supervision

- Annex I – Large enterprises^(a)
- Digital infrastructure including Qualified trust service providers, TLD name registries, DNS service providers
- Public administration of central government
- Operators of essential services
- Member State selected entity^(c)



Important | Reactive supervision

- Annex I – Medium enterprises^(b)
- Annex II – Large & Medium enterprises
- Member State selected entity^(c)

(a) Large enterprises: >€50m annual revenue; 250+ employees

(b) Medium enterprises: >€10m annual revenue; 50+ employees

(c) Member State selected: Any size; selected based on risk profile

Journey of NIS2

Committee Assignment:

Within the European Parliament, the NIS2 file was assigned to the **Committee on Industry, Research, and Energy** to shape the directive and ensuring its alignment with cybersecurity objectives.

Committee Adoption:

On **October 2021**, the committee adopted its report on NIS2 outlining key provisions and recommendations related to cybersecurity capabilities and resilience.

Council Position:

The **Council** (representing EU member states) agreed on its position regarding NIS2 on **December 2021**.

Provisional Agreement:

The **co-legislators** (European Parliament and Council) reached a **provisional agreement** on the NIS2 text on **May 2022**.

Formal Adoption:

The conclusion step in the legislative process was done when the **political agreement** reached by the Parliament and the Council was **formally adopted** in **November 2022**.

Entry into Force and Transposition:

NIS2 entered into force on **16 January 2023**.
EU member states have until **17 October 2024**, to transpose NIS2 measures into their national law.

DORA (ACT) vs NIS2 (DIRECTIVE)

Regulation: DORA is a **regulation**, meaning it applies unchanged in all EU countries upon entry into force (scheduled for January 17, 2025).

Binding: It is a **binding legislative act** that must be enforced in its entirety.

Applicability: DORA specifically targets the financial sector, enhancing digital operational resilience.

Lex Specialis: DORA takes precedence over NIS2 for the financial sector.

Directive: NIS2 is a **directive**, requiring transposition into national law by each EU country.

Transposition Deadline: Member States have until October 2024 to transpose NIS2 into their national legal frameworks.

Nuances: Entities subject to NIS2 may experience nuances based on national transposition.

How to be NIS2 Compliant

Article 20: Governance

Article 21: Cybersecurity Risk Management Measure

Article 23: Reporting Obligations

Article 24: Use of European cybersecurity certification schemes





Essential Entities:

Max (10 MEUR, 2% of total worldwide annual turnover)

Important Entities:

Max (7 MEUR, 1.4% of total worldwide annual turnover)

**Financial
Impact on
Organization:
Penalties**

- The management bodies of **essential and important organizations** approve the cybersecurity risk management measures taken by those organizations to comply with Article 21, oversee the implementation of those measures and can be held liable for infringements of the Article.
- The management bodies are required to follow training and are encouraged to offer similar training to their employees on a regular basis. This way, employees gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the organization.



Article 20: Governance

- Essential and important organizations should take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems. Proportionality is based on the organization's exposure to risk, the organization's size and the likelihood and severity of possible incidents, including the economic and societal impact.
- Essential and important organizations should take an all-hazard approach to be prepared for a full spectrum of incidents and emergencies and be able to protect network and information systems and the physical environment of those systems. The measures should include at least the following:
 - Risk analysis & information security policies;
 - Incident handling;
 - Business continuity;
 - Supply chain security
 - Vulnerability handling and disclosure;
 - Procedures to assess the effectiveness of cyber risk management;
 - Computer hygiene practices and cybersecurity training;
 - Policies and procedures for cryptography and encryption;
 - Human resources security, access control policies and asset management;
 - Use of multi-factor authentication and secure communication systems.



Article 21: Cybersecurity risk management Measures

- Essential and important organizations should notify the CSIRT or, where applicable, the competent authority in case of a significant impact on the provision of their services.
- In case of a significant cyber threat, the organizations need to inform the recipients of their services that are potentially affected on any measures or remedies that they can take in response to the threat. Where appropriate, entities can inform recipients on the threat itself.

The organizations are required to submit to the CSIRT or competent authority:

- a. Within 24 hours of becoming aware of the significant incident, an early warning, which shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- b. Within 72 hours of becoming aware of the significant incident, an incident notification, which shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, and the indicators of compromise;
- c. Upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
- d. A final report not later than one month after the submission of the incident notification under point (b).



Article 23: Reporting Obligations


- To demonstrate that the security obligation of requirements of Article 21 is met, Essential and important organizations should use specific ICT products, services and processes that are certified under European cybersecurity certification schemes.
- Essential and important organizations should use qualified trust services.



Article 24: Use of European cybersecurity certification schemes

Compliance by Using Certification

	NIS2 requirements for critical entities; Articles 20 & 21	Leverage established standards such as IEC 62443
Governance & Process	<ul style="list-style-type: none"> • Risk analysis & information system security policies • Assess effectiveness of cyber risk management • Business continuity 	<ul style="list-style-type: none"> • Policies and procedures • Risk Management • Disaster recovery and business continuity • Security requirements • Reference network architecture
Organization & People	<ul style="list-style-type: none"> • Management board approves and oversees the cyber risk management approach • Computer hygiene practices and cybersecurity training • Supply chain security 	<ul style="list-style-type: none"> • Roles and Responsibilities • Security training • Third parties • Asset inventory
Technology & Security capabilities	<ul style="list-style-type: none"> • Incident handling • Cryptography and encryption • Vulnerability handling and disclosure • Access control policies and asset management • Use of multi-factor authentication and secure communications systems 	<ul style="list-style-type: none"> • Network segmentation • Patch and vulnerability management • Remote access security



Establish a baseline: by conducting assessments to gain insights into an organization's cybersecurity risks. By using internationally recognized frameworks and standards, such as the IEC 62443, Cybersecurity Capability Maturity Model (C2M2) and the CRA, these assessments can be conducted effectively in a standardized manner.

Develop a Strategic Plan: The insights gained during the assessment can be used to develop short- and long-term action plans to address identified risks and vulnerabilities.

Promote Ownership and Accountability: Under NIS2 all incidents within a defined threshold will have to be reported. Assigning risk ownership is precisely what is required

The Approach

- **Cybersecurity Awareness Program**
- **Business Continuity and Disaster Recovery Planning**
- **ISMS Implementation**
 - Incident handling
 - Procedures to assess the effectiveness of cyber risk management
 - Supply chain security
 - Vulnerability handling and disclosure
 - Human resources security, access control policies and asset management
 - Use of multi-factor authentication and secure communication systems
- **Cyber Policy Design**
 - Risk analysis and information security policies
 - Policies and procedures for cryptography and encryption
- **Cyber Maturity Assessments & Strategic Roadmap**



Actions for Quick Wins in NIS2 Compliance

How to be DORA Compliant



Remember about DORA

- DORA applies to over 22,000 financial entities and ICT service providers in the EU.
- The regulation introduces specific and prescriptive requirements for all financial market participants, including e.g., banks, investment firms, insurance undertakings and intermediaries, crypto asset providers, data reporting providers, and cloud service providers.
- DORA introduces an end-to-end holistic framework for effective risk management, ICT and cyber security operational capabilities, and third-party management to assure the consistent delivery of services along the entire financial value chain.
- DORA's five key pillars: ICT Risk Management, ICT-related Incident Management, Digital Operational Resilience Testing, ICT Third Party Risk Management, and Information Sharing.
- The regulation is unique in introducing an EU-wide oversight framework on critical ICT third-party providers, as designated by the European Supervisory Authorities (ESAs)

Pillars of DORA

ICT Risk Management

Minimize ICT risk through granular risk identification and treatment

Embed ICT risk management in organizational structure

Develop comprehensive ICT risk management framework

Regularly test response and recovery

Classification and Reporting of ICT-Related Incidents

Establish incident management process

Develop capabilities to monitor, mitigate and follow-up incidents

Classify incidents according to defined factors

Report major incidents to the relevant competent authority

ICT Third-Party Risk Management

Integrate third-party risk within the risk management framework

Adopt and review third-party risk management risk strategy

Maintain inventory of all contractual agreements with ICT service providers

Require third-party risk assessments

Digital Operational Resilience Testing

Implement an operational resilience testing programme

Test using independent parties

Perform annual tests for critical ICT systems and applications

Information Sharing Between Financial Entities

Share cyber threat information and intelligence

Exchange information to enhance operational resilience

A Stronger mandate for ESAs



Under the DORA provisions, European Supervisory Authorities (ESAs) will play a vital role in the overall market's digital resilience. Financial businesses can expect higher supervision from ESAs and more robust controls, with obligations such as:

- Defining policies
- Implementing a mature risk management framework
- Sharing mandatory reporting for ICT-related incidents
- Designing robust continuity and disaster recovery plans
- Performing mandatory and advanced resilience testing, including:
 - A mandatory annual internal testing* with the financial institutions providing the findings report to the ESAs. Advanced testing** at least every 3 years by an external entity: this will allow ESAs to issue a certificate stating the company's compliance regarding penetration testing.

*Applicable to all actors in the financial sector. ** Applicable to companies with specific criteria

DORA Applicability

Financial Entities

- Credit institutions
- Payment institutions
- Electronic money institutions
- Investment firms
- Crypto asset service providers
- Trading venues
- Insurance undertakings
- Institutions for occupational retirement provision

ICT Third-Party Service Providers

- ICT third-party service provider means an undertaking providing ICT services
- ICT services means digital and data services provided on an ongoing basis
- Critical ICT third-party service provider

Recurring Compliance Themes in EU Legislation

The DORA regulation is a piece of the strategy “A Europe fit for the Digital Age” includes over 14 regulatory initiatives to shape Europe’s digital future over the next decade. These regulations share five recurring themes that refer to the General Data Protection Regulation (GDPR).

- **Reporting:** notification requirements in case of an incident, data breach, or any other event to the supervisory authorities, affected users and clients.
- **Documentation:** obligation to record and keep documentation, archives, and records for logging information and activities including all significant cyber threats, which will require a more mature incident management capability to monitor, mitigate, and resolve cyber incidents.
- **Third-party management:** The laws raise the bar for how businesses work with third parties and how much responsibility they retain, including: accountability for further control over suppliers or business partners, being responsible to establish contracts regulating the relationship with third parties with a minimum set of details to comply with DORA, and having a well-defined ICT third-party risk management plan.
- **Governance:** obligations relating to organizational and governance procedures that guarantee efficient risk management and regulatory compliance, including having an internal governance and control framework to ensure efficient management of ICT risks, documenting the process and reviewing them at least once a year or in the event of significant ICT-related occurrences, ICT auditors ought to perform routine audits of the management framework.
- **Assessments:** DORA requires financial institutions to analyze the risk associated with their outdated ICT systems periodically. Moreover, risk evaluations will be necessary for any outsourcing agreements that support the delivery of crucial or significant functions

The Approach

- **Scope and identify overlaps:** Determine the organization's risk appetite and identify the threats it currently confronts. Prioritize the required actions based on gap between the current policies, processes, and defences, and the required ones.
- **Understand your environment:** Understanding possible risks and threats requires clear and consistent visibility into your infrastructure, whether on-premises or in the cloud. Businesses can find areas that can be improved with vulnerability scanning, penetration testing, and red team exercises.
- **Understand the changes to your environment:** In addition to potential external attackers, consider internal developments that could halt or break a system. To prevent errors from paralyzing an entire organization, put in place configuration change management and file integrity monitoring.
- **Automation:** Automate tedious and intricate security procedures to better manage funds, time, and resources to ensure compliance.
- **Business continuity and resilience:** Although prevention is crucial, organizations cannot wholly prevent compromises. Businesses must be ready to respond if something gets past security measures. How financial institutions prepare for such an incident is a crucial question. It is critical to how quickly businesses bounce back. To be resilient is to be able to survive an attack and quickly and effectively recover.
- **Information sharing:** Sharing information can help reduce the work involved in spotting threats. Financial organizations can be better prepared by using the lessons learnt by other businesses in the industry. Information exchange should be used as valuable threat intelligence to lessen the continuous effect on the compliance and security teams

Actions for Quick Wins in DORA Compliance

Realize what's at stake Recognize what has to be done, the situation as it stands, and the active projects. Financial businesses can then start carrying out their plans based on this image. Understanding that compliance, like security, will always be ongoing is crucial.

Identify internal risks: Businesses should pay attention to employees' mistakes, even though external attacks are the more evident component of the equation. An employee may open a malicious attachment or click on a malicious link due to inattention. Making security a continual presence—technically and logically—is the best approach to avoid this.

Focus on your supply chain: Be aware of the risks partners and suppliers pose, particularly those related to software and applications. The best way to do this is to thoroughly examine these partnerships to ensure they adhere to the standards of the hosting company.

Discover hidden vulnerabilities: Invest heavily in vulnerability scans and pen tests to maintain compliance and implement effective risk management. The real-world effects that might not be realized in a risk assessment can be found through pen tests and vulnerability scans. The results of these scans and tests can also be used to reprioritize jobs and projects since they give a more accurate picture of what can occur if an attacker takes advantage of these risks.

Train your employees: Prioritize training their staff members on security awareness. Avoid overburdening people with acronyms and technical jargon by concentrating on one subject per month. The information must relate to the employees' day-to-day activities.

Build layers of defence: Training is enormously influential. However, businesses need additional layers of protection to fortify the organization against evolving threats. These technology layers can help detect phishing emails, ransomware, and malware and prevent an attack from crippling the infrastructure or the ability to do business.



Thank you

**Dr. Leila Taghizadeh, Global Head of Cyber Risk
Management & CISO @Allianz**

<https://www.linkedin.com/in/leilataghizadeh/>