ADACOM NIS2 Playbook

From Legislation to Resilience

A Consulting Service from

ADACOM

SECURITY BUILT ON TRUST

ADACOM
SECURITY BUILT ON TRUST

About ADACOM

ADACOM, a member of IDEAL Holdings, is an Established, Leading Provider of Trust Managed Services and a Cybersecurity Services Integrator headquartered in Athens, Greece, with subsidiaries in Cyprus and the Kingdom of Bahrain.

The company has a strong presence in more than 30 countries across the EMEA region. For nearly 25 years, it has enabled its clients to operate in a modern and secure manner, helping them digitize business processes and provide reliable identity assurance. By leveraging international expertise through global partnerships and local presence, ADACOM delivers tangible results against internal or external threats and addresses every cybersecurity challenge.

Today, more than 500 organizations trust ADACOM to protect and secure their data along with the safety of their businesses.

Executive Summary

The Joint Ministerial Decision (JMD) 1689/2025 is a cornerstone of Greece's national cybersecurity framework, issued under Law 5160/2024, which formally transposes the EU NIS2 Directive (Directive (EU) 2022/2555) into Greek law. Aimed at strengthening the cyber resilience of essential and important entities across both public and private sectors, the JMD introduces structured obligations around governance, risk management, incident reporting, and accountability. Organizations operating in energy, transport, healthcare, digital infrastructure, and other critical domains must now comply with a higher standard of cybersecurity readiness—under close supervision by national authorities.

This eBook offers a practical roadmap for understanding the NIS2 objectives and the concrete obligations introduced by JMD 1689/2025. It outlines what's expected from businesses, highlights common compliance gaps, and offers actionable guidance on how to meet and exceed these regulatory obligations. By leveraging ADACOM's strategic expertise and services, organizations can turn compliance into a competitive advantage and build a resilient cybersecurity posture for the years ahead.

Disclaimer

This guide is provided exclusively for informative and advisory purposes and does not constitute legal, regulatory, or professional advice of any kind. Its content aims to offer a general overview of the requirements of the NIS2 Directive and Hellenic Ministerial Decision 1689/2025, without constituting an official interpretation of the applicable legislation.

Organizations bear full and sole responsibility for their full compliance with the applicable provisions and obligations, and are encouraged to consult specialized legal and/or technical advisors for the provision of personalized advice tailored to their specific needs and operating conditions.

Contents

Introduction

The Joint Ministerial Decision (JMD) 1689/2025 is a cornerstone of Greece's national cybersecurity framework, **The European Union's NIS2 Directive (Directive (EU) 2022/2555) represents a significant step forward in harmonizing cybersecurity measures across Member States.** The primary objective of NIS2 is to ensure a high common level of cybersecurity across the EU by imposing obligations on entities that provide essential and important services. These obligations encompass risk management, incident reporting, and the implementation of appropriate technical and organizational measures.

In Greece, this Directive has been transposed into national law through Law 5160/2024, with further specifications outlined in Joint Ministerial Decision (JMD) 1689/2025. The recent Joint Ministerial Decision (JMD) 1689/2025, published in the Government Gazette B' 2186 on May 6, 2025, significantly changes how businesses and public entities must address the security of their digital infrastructures.

JMD 1689/25: An Overview

The NIS2 Directive replaces the NIS Directive (2016) by introducing broader obligations, stricter enforcement mechanisms, and a more comprehensive scope. Its goal is straightforward but ambitious: to ensure a high standard level of cybersecurity across the EU, particularly in the face of rapidly evolving digital threats and interconnected risks.

While the first NIS Directive focused mainly on critical infrastructure and digital service providers, NIS2 applies to a broader range of sectors. It introduces detailed requirements for both essential and important entities. It recognizes that disruptions in many industries can now have systemic impacts on society, public safety, and the economy.

Who Needs to Comply?

NIS2 expands its scope, encompassing more critical sectors, from 7 to 18, than its predecessor. Entities are classified based on the criticality of their services. The new national cybersecurity requirements framework includes technical, operational, and organizational measures for cybersecurity risk management, as provided in paragraph 2 of Article 15 of Law 5160/2024, as in force.

It addresses two main categories of entities, Essential and Important, as defined in Article 4 of Law 5160/2024, and aims to protect networks and information systems from cyber threats. The distinction between "essential" and "important" entities is particularly significant, as the former are subject to stricter requirements.

However, all entities falling within the scope of the JMD are called upon to adapt to a new environment with increased compliance requirements.

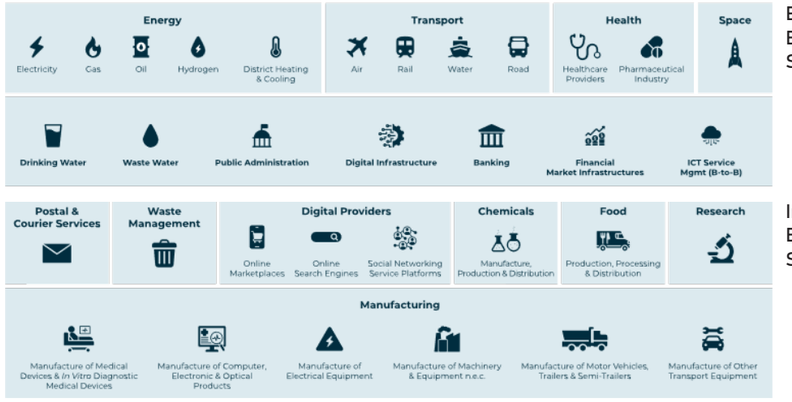

Image 1: NIS2 Entities (https://www.datacore.com/blog/nis2-directive/)

Back to Contents

This classification helps define the level of oversight and type of obligations that each must meet. The obligation for a comprehensive cybersecurity risk management program is at the center of the new framework. Under the responsibility of the supreme management body, each entity must develop and implement such a program that will include policies, procedures, roles, and responsibilities, as well as technical, organizational, and operational security measures.

Overall, organizations operating within these sectors must meet cybersecurity obligations because of the disruptions' risks and because their operational integrity is critical to national and EU-level security and economic stability.

A Focus on Accountability

One of the most consequential changes introduced by NIS2—and further detailed in Greece's Joint Ministerial Decision 1689/2025—is the strong emphasis on accountability at the leadership level. Gone are the days when cybersecurity was considered the sole domain of IT departments. JMD 1689/2025 brings to the forefront the role and responsibility of senior management. The supreme management body of each entity is responsible for approving the cybersecurity risk management program and its overall implementation, supervision, periodic evaluation, and continuous improvement.

Under the Directive, board members and executive leadership are directly responsible for ensuring that their organizations adopt and implement effective cybersecurity risk management strategies. This includes:

- Overseeing governance structures for cybersecurity.
- Ensuring that appropriate resources, financial, technological, and human, are allocated.

- Participating in or facilitating training programs that build cybersecurity literacy at the top.
- Being held liable in cases where negligence or non-compliance leads to significant incidents.

The shift toward executive accountability reflects growing recognition that cybersecurity is not just a technical issue: it's a business risk with legal, reputational, and operational implications. For many organizations, this shift will require a cultural change, embedding cybersecurity considerations into core strategic planning and leadership conversations.

In Greece, this obligation is further cemented through the JMD, which explicitly requires a well-documented cybersecurity general policy and discrete thematic policies covering specific aspects of cybersecurity. The JMD defines at least eleven thematic policies that must be developed, from access control and asset management to data encryption and supply chain security.

Additionally, entities under the JMD must maintain an accurate inventory of information assets hosted in their facilities and the cloud and be continuously supervised by designated executive stakeholders. The entity must implement procedures for monitoring and evaluating compliance with its regulatory obligations, the results of which must be periodically submitted to the supreme management body.

Moreover, the JMD confirms the obligation to appoint an Information and Communication Systems Security Officer (ICSSO) in each entity. The ICSSO reports directly to the entity's supreme management body on matters related to cybersecurity. It should be noted, though, that the duties of the ICSSO are incompatible with those of the Data Protection Officer (DPO), according to paragraph 5 of article 15 of Law 5160/2024.

By making leadership accountable, cybersecurity is no longer reactive or siloed. It becomes a shared, strategic responsibility with visible governance, measurable performance, and clearly defined roles at every level, from IT administrators to boardrooms.

Back to Contents

Implementation Requirements per Joint Ministerial Decision 1689/2025

JMD 1689/2025 outlines specific measures that entities must implement to comply with the national transposition of NIS2. These measures are designed to enhance organizations' cybersecurity posture and ensure the resilience of critical services.

The key requirements of the JMD 1689/2025 emphasize the importance of a proactive and comprehensive approach to cybersecurity, integrating technical measures with organizational governance. These requirements are summarized in the following matrix:

Requirement Category	Specific Obligations
Governance and Accountability	• Appoint a dedicated Information and Communication Systems Security Officer (ICSSO) • Develop and submit a comprehensive cybersecurity policy to the National Cybersecurity Authority • Maintain an up-to-date inventory of information and communication assets
Risk Management	• Conduct regular risk assessments and implement appropriate mitigation measures • Ensure business continuity and disaster recovery planning • Implement supply chain security measures
Incident Reporting	• Report significant incidents to the National CSIRT within 24 hours • Notify affected service recipients as appropriate
Training and Awareness	• Provide annual cybersecurity training for all employees • Ensure management participates in specialized training programs
Compliance and Monitoring	• Undergo regular audits by the National Cybersecurity Authority • Implement corrective actions as directed by supervisory authorities

Table 1: JMD 1689/2025 Requirements

Back to Contents

Among the core implementation requirements introduced by Joint Ministerial Decision 1689/2025, one of the most critical elements is the designation of an Information and Communication Systems Security Officer (ICSSO). However, organizations must understand that appointing someone to this role is not simply a procedural formality. The real value lies not in the existence of the title but in the actions and responsibilities that come with it.

The ICSSO is entrusted with executing and overseeing concrete cybersecurity operations. These include conducting periodic cyber risk assessments, performing internal security audits, coordinating incident response strategies, and leading administrative security reviews. In other words, the ICSSO must be operationally active—regularly engaging with systems, people, and processes—not just listed on the org chart. A passive or symbolic assignment undermines the law's intent and the organization's resilience.

> "The role of the Information and Communications Systems Security Officer (ICSSO) is very important. It is also important to understand that it is not enough to understand the role, but also the obligations and actions that this role is responsible for. In other words, it should be understood that the essence is for the ICSSO to carry out security processes, such as cybersecurity risk assessments, cybersecurity audits, administrative reviews from this role, and not simply exist in the organizational chart."
>
> **Panagiota Lagou,**
> GRC Director at ADACOM

For many organizations, this requires a mindset shift. It's no longer enough to say, "we have someone in charge." The expectation is that the ICSSO will act as the functional engine behind the security management system, translating policy into practice and ensuring that cybersecurity becomes a living, evolving part of the business. As regulators increase their scrutiny, and cyber threats continue to escalate, the role of the ICSSO will be instrumental not just for compliance—but for maintaining operational integrity and stakeholder trust.

What are the Shortfalls of the JMD 1689/25?

While Joint Ministerial Decision 1689/2025 provides much-needed clarity and structure for organizations navigating the NIS2 regulatory landscape, it has its limitations. One of the key concerns raised by cybersecurity subject matter experts is that the JMD 1689/2025 outlines a set of specific policies and procedures, but these do not comprehensively address all areas of cybersecurity governance. In other words, while the regulation offers a clear path forward, it should be viewed as a directional guide, not a complete blueprint. Organizations that treat it as the final word on cybersecurity obligations may find themselves exposed to areas not explicitly covered, particularly in domains like strategic governance, continuous risk monitoring, or advanced threat detection.

Another critical gap lies in the insufficient separation of roles between the ICSSO and the IT department. Although the JMD 1689/2025 rightfully distinguishes between the ICSSO and the Data Protection Officer (DPO), acknowledging the distinct nature of privacy versus security responsibilities, it fails to define a clear boundary between cybersecurity governance and day-to-day IT operations. This lack of separation can blur accountability lines and create potential conflicts of interest. For instance, critical weaknesses may go unreported or unresolved if the same department is responsible for running systems and auditing their security. For cybersecurity to be effective and trusted, especially under the heightened accountability model of NIS2, segregation of duties must be clearly defined and enforced.

Back to Contents

ADACOM
SECURITY BUILT ON TRUST

How can Businesses go Above and Beyond the Ministerial Decision?

Simply meeting the minimum requirements of JMD 1689/2025 isn't enough to truly future-proof your organization and ensure operational continuity. Organizations need an expert ICSSO with strategic cybersecurity insight and hands-on experience to guide them through the technical and organizational complexities of compliance. This means not only identifying and communicating cyber risks promptly but also advising on the right mix of controls, from network segmentations and multi-factor authentication to governance frameworks tailored to your threat landscape, business operations, and best-practice standards.

That's precisely where ADACOM steps in. As a Qualified Trust Service Provider (QTSP) and a leading Cybersecurity Integrator and Managed Security Services Provider, ADACOM brings both strategic consulting and operational support to organizations facing JMD 1689 compliance.

> "They should have a ICSSO with the expertise to guide the Organization on cybersecurity issues, technically and organisationally, to identify and report risks in a timely and adequate manner, and to advise on appropriate technical and organisational measures, taking into account the organisation's mode of operation, the threat environment and best practices."
>
> **Panagiota Lagou,**
> GRC Director at ADACOM

Their key offerings include:

- **Governance & Consulting:** The JMD 1689/2025 requires organizations to appoint an ICSSO and ensure they can perform duties like risk assessments, administrative reviews, and cyber policy development. ADACOM provides expert guidance to define, structure, and operationalize the ICSSO role, ensuring your appointed officer is empowered and equipped to drive risk assessments, audits, incident response, and administrative reviews, per JMD obligations.

- **Managed Security Services:** Η ΚΥΑ επιβάλλει δυνατότητες συνεχούς παρακολούθησης, ανίχνευσης και αντίδρασης. Το SOC της ADACOM παρέχει συνεχή ανίχνευση απειλών, διαχείριση περιστατικών σε πραγματικό χρόνο και Threat Intelligence που τροφοδοτείται από AI, βοηθώντας σας να διατηρήσετε επαγρύπνηση και ανθεκτικότητα σε on-premise, cloud και υβριδικά περιβάλλοντα.

- **The JMD mandates continuous monitoring, detection, and response capabilities.** ADACOM SOC delivers continuous threat detection, real-time incident management, and AI-powered Threat Intelligence, helping you maintain vigilance and resilience across on-premise, cloud, and hybrid environments.

- **Incident Response & Assurance:** Organizations must be able to respond to and report incidents within strict timeframes and test their processes. ADACOM offers incident response planning, tabletop exercises, penetration testing, and compliance audits, all necessary for demonstrating readiness and responsiveness.

- **Trust Services & PKI:** While not explicitly mentioned in the JMD 1689/2025, using qualified trust services, digital signatures, and secure communication mechanisms is strongly implied as a best practice for identity and data integrity. As a QTSP certified under eIDAS and ISO standards, ADACOM offers PKI infrastructure, digital certificates, and signing solutions essential for securing communications and identities and ensuring integrity across systems.

- **Training and Awareness Programs:** The JMD 1689/2025 mandates annual cybersecurity training for employees and management. ADACOM provides tailored cybersecurity training programs for both technical teams and executive leadership, ensuring organizations meet their ongoing awareness obligations.

How ADACOM helps

The following table provides a mapping of the ADACOM services and solutions to the JMD 1689 requirements.

ADACOM Service	Supports JMD 1689 Requirement
Governance & Consulting	ICSSO role setup, policy development, risk governance
Managed Security Services (SOC)	Real-time monitoring, threat detection, and response
Incident Response & Assurance	Incident handling, reporting, testing, and audits
Trust Services & PKI	Secure communication, authentication, and data integrity
Training Programs	Employee & executive cybersecurity awareness

Table 2: Summary of ADACOM's services to support JMD 1689 Requirements

As organizations in Greece work to align with the demands of the Joint Ministerial Decision 1689/2025, it is clear that compliance is not a one-time task; it's an evolving journey that requires strategic oversight, operational rigor, and continuous improvement. Navigating these regulatory requirements effectively demands more than technical fixes; it requires a governance-first mindset and expert guidance.

ADACOM's specialized consulting and cybersecurity governance services are designed to help organizations meet their obligations, build long-term cyber resilience, and gain a dedicated cybersecurity governance ecosystem. From role definition and policy development to risk assessments and board-level accountability, our team of experts is ready to support your compliance strategy. This means the ICSSO has the framework and tools to act decisively, consistently identify and remediate vulnerabilities, and your

organization stays one step ahead of evolving threats.

ADACOM's solutions and services allow organizations to meet the requirements of JMD 1689 and comply with the mandates of NIS2. The following table provides a high-level mapping of ADACOM's services with NIS2 requirements.

ADACOM Solution/Service	NIS2 Reference
Digital Risk Protection & Vendor Risk Assessment	Article 21 -- para. 2(d) Article 21 -- para. 2(e) Article 23
Incident Readiness	Article 20 Article 21 -- para.2(b) Article 21 -- para. 2(e) Article 21 -- para. 2(f) Article 21 -- para. 2(g)
Privileged Access Management	Article 21 -- para. 2(g) Article 21 -- para. 2(i) Article 21 -- para. 2(j)
Breach & Attack Simulation / Autonomous Penetration Testing	Article 21 -- para. 2(e)
Web Application Scanning	Article 21 -- para. 2(e)
Security Awareness Training	Article 20 Article 21 -- para. 2(g)
Phishing Campaigns Management System	Article 20 Article 21 -- para. 2(g)
Cloud Native Protection	Article 21 -- para. 2(d)
Cloud Access Security Broker	Article 21 -- para. 2(d)
Web Application Firewall	Article 21 -- para. 2(d)
Identity Management & Strong Authentication	Article 21 -- para. 2(g) Article 21 -- para. 2(i) Article 21 -- para. 2ju)
Configuration Management	Article 21 -- para. 2(e) Article 21 -- para. 2(g)

Table 3:Mapping of ADACOM's solutions and services with NIS2 requirements

Back to Contents

ADACOM Solution/Service	NIS2 Reference
Network Security	Article 21 -- para. 2(e) Article 21 -- para. 2(g)
Malware Protection	Article 21 -- para. 2(g)
Monitoring & Alerting as-a-Service	Article 21 -- para. 2(b) Article 21 -- para. 2(c) Article 21 -- para. 2(e) Article 21 -- para. 2(g)

Table 3:Mapping of ADACOM's solutions and services with NIS2 requirements

ADACOM
SECURITY BUILT ON TRUST

Contact ADACOM today to schedule a consultation and take the next step toward secure, sustainable, trustworthy, and regulation-ready operations.

Contuct us

Greece / HQs
25 Kreontos Str.
104 42, Athens - GR
+30 210 51 93 700
info@adacom.com

Greece / Thessaloniki
8 Halkis Str., 555 35 Pylea
Thessaloniki - GR
+30 2310 365 250
info@adacom.com

Cyprus
10 Katsoni Str.,
1082 Nicosia - CY
+357 22 444 071
infocy@adacom.com

Kingdom of Bahrain
Manama Center, Blog: 316
Road: 383, Building: 128 Flat/
Office: 2030
info@adacom.com