TWELVESEC

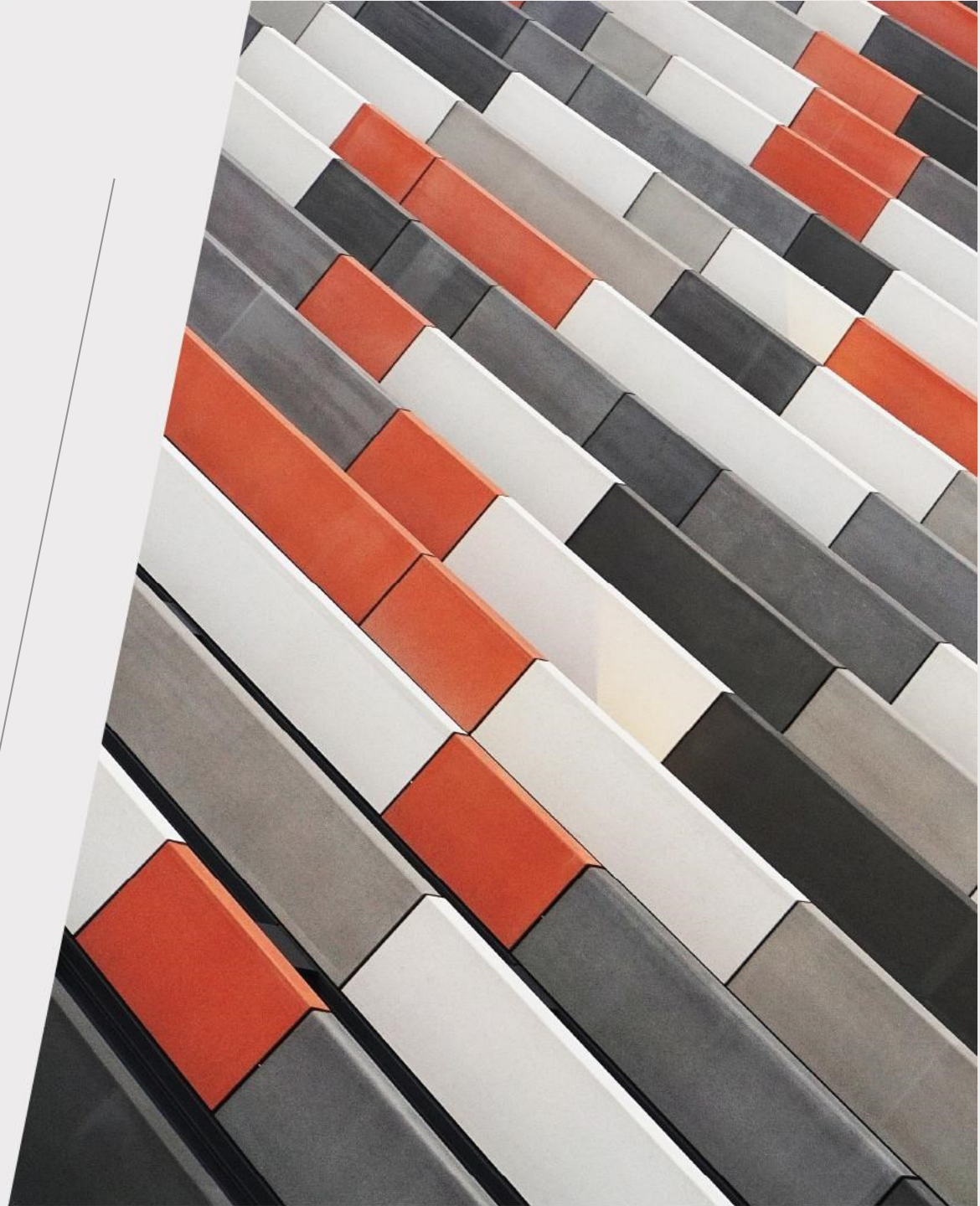
Your Partner in Cyber Security

Understanding NIS 2; Impact on Greek Companies

Key Implications, Requirements, and Greek Transposition

Yiannis Koukouras
Managing Director at TwelveSec

www.twelvesec.com
hello@twelvesec.com



Presenter

Yiannis Koukouras

- Managing Director at TwelveSec
- MSc Computer Systems Security
- Penetration Tester / Security Consultant since 2004
- CISSP, CISSP-ISSAP, CDPSE, CISM, CISA, OSCP
- (ISC)2 Hellenic Chapter Honorary Member
- Coach of the National Hacking Team (2015-2016)

Also:

- D&D DM
- Skipper
- Musician
- Windsurfer
- Dad Joker

Agenda

- What is NIS2?
- Am I affected?
- What should I do?
- References

History Repeats

England circa 1350 - 1550

Byzantine empire 7th – 10th century

What is NIS2?

What is NIS 2?

The NIS 2 Directive (EU Directive 2022/2555) is a European Union regulation aimed at strengthening cybersecurity across the European Union.

- It replaces the NIS Directive (2016/1148), expanding the sectoral scope and establishing penalties and new rules on supply chain resilience, and incident reporting.
- It sets out mandatory cybersecurity requirements for large and medium-sized, essential and important entities within the EU, including private and public sectors.
- It fosters cooperation among Member States in cybersecurity matters by establishing a network of CSIRTS, and a European Cyber Crisis Liaison Organization Network.

Timeline for Transposition and Compliance

November 2022

The NIS 2 Directive was officially adopted by the European Parliament, enhancing cybersecurity regulations.

January 2023

Preliminary compliance measures are finalized in Greece, preparing for full implementation.

October 2024

The NIS 2 Directive came into effect, marking the start of compliance preparations for member states.

October 2024 Onwards

Post-transposition compliance measures are enforced, requiring adherence to operational security protocols.

November 2024

Deadline for EU member states, including Greece, to transpose the NIS 2 Directive into national law.

Ongoing

Continuous monitoring by the European Commission to ensure compliance and address any transposition delays.

NIS 2 – Purpose and Goals

- To enhance the resilience of critical infrastructure against cyber threats.
- To secure critical networks and information systems in the EU.
- To ensure that both large and medium-sized enterprises adopt rigorous protocols to mitigate risks.
- It affects a wide range of industries including Energy, Transport, Health, Finance, Water, Digital Infrastructure, and Public Administration.

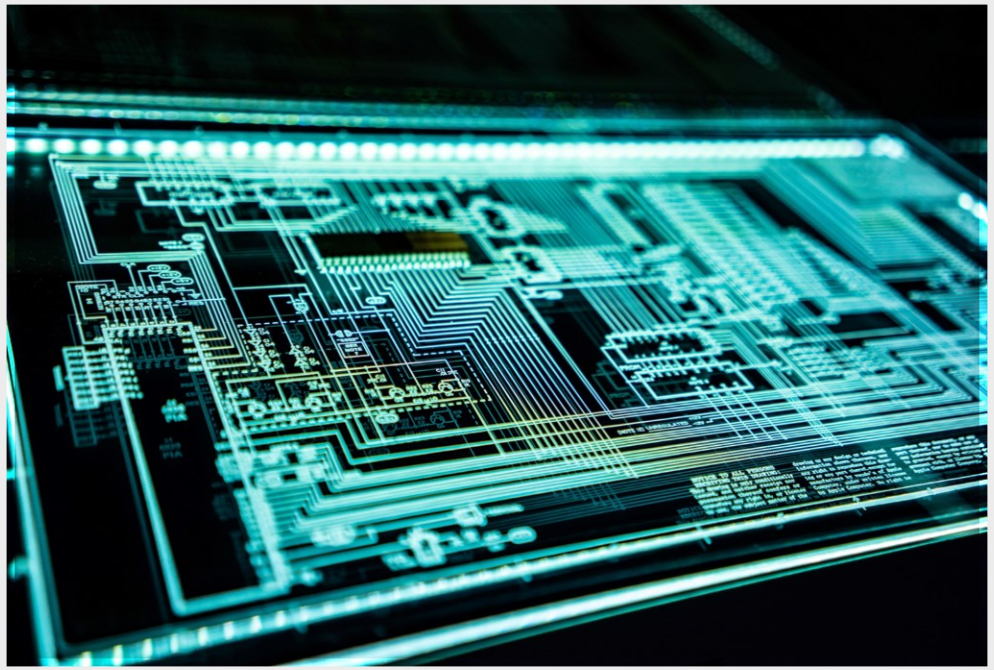
The directive represents a significant step towards a more secure digital environment in Europe.

- Greece transposed the NIS 2 Directive through **Law 5160/2024**.
- The **Hellenic Cybersecurity Authority (HCA)** is tasked with overseeing the implementation and enforcement of NIS 2 in Greece.

Key Provisions in Greek Law:

- Introduction of new **cybersecurity obligations** for critical sectors.
- Defined **incident reporting** procedures and timelines.
- Creation of **risk assessment frameworks** for companies within critical infrastructure sectors.
- Development of guidelines for **collaboration** between public and private sectors on cybersecurity resilience.
- **Self Registration** needs to take place by **28th of March 2025** for all entities under Art. 19(1) of the Greek Law, and by **11th of April 2025** for all other entities (both essential and important) via email at **register.ncsa@cyber.gov.gr**.
- **Compliance Reviews**: Regular reviews and compliance checks starting **2025**.

Why is NIS 2 Important for Greek Companies?



- **Impacts:** Critical sectors such as Energy, Transport, Finance, and Digital Infrastructure.
- Greek businesses in these sectors will have to comply with **stricter cybersecurity measures**.
- The **Hellenic Cybersecurity Authority (HCA)** is the key regulator in Greece for the implementation of NIS 2.
- Greek companies will need to meet **new obligations** regarding cybersecurity.

Penalties for Non-Compliance

Non-compliance with the NIS 2 Directive can result in fines up to 10 million euros or 2% of global turnover, emphasizing the importance of adherence.

Breaches may result in penalties for management, including liability and a potential temporary ban from management roles.

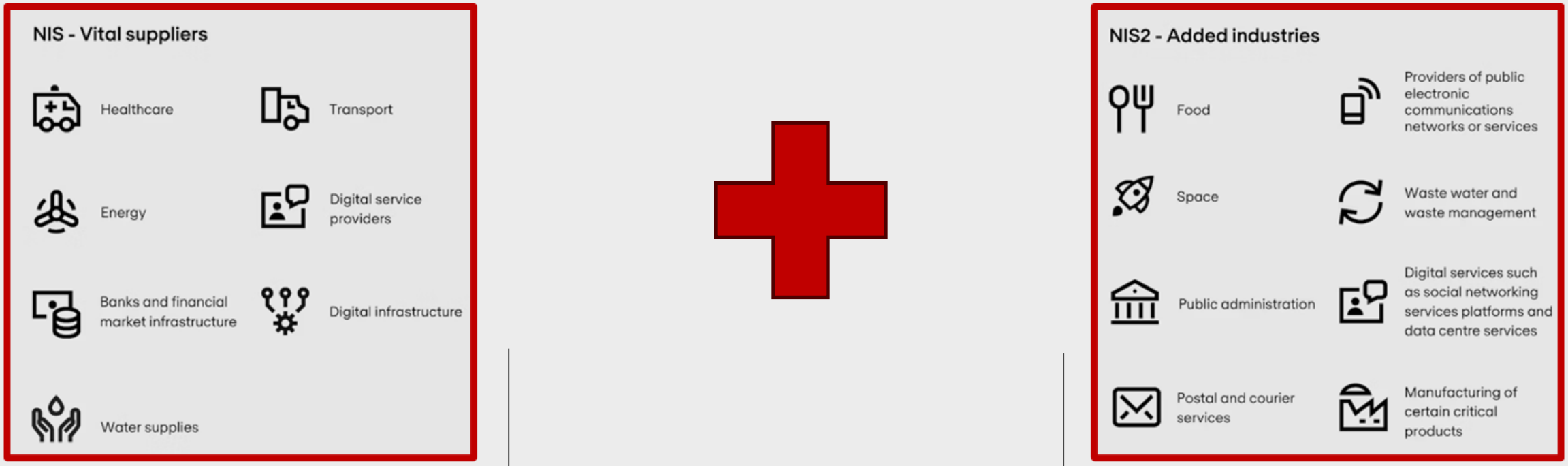
Operational restrictions may take place for non-compliant businesses.

Penalties are determined based on negligence, violation severity, and cooperation during investigations, ensuring a fair and just enforcement process.

National Supervisory Authorities are empowered to conduct audits and enforce compliance, playing a crucial role in maintaining cybersecurity standards across sectors.

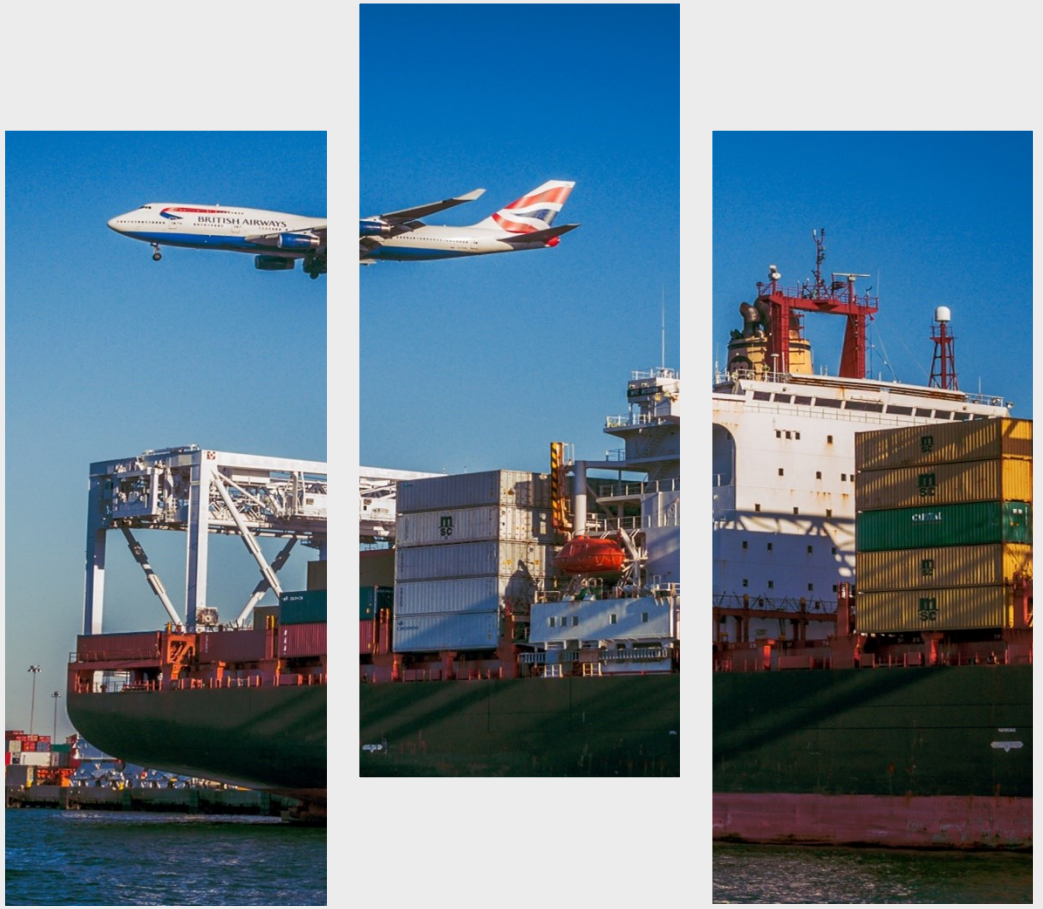
Am I Affected?

NIS 2 – Impacted Sectors



Essential vs. Important Entities

- Essential Entities must operate in critical sectors, employing over 250 individuals or generating annual revenues exceeding €50 million, ensuring their significant role in societal stability.
- Essential Entities face stringent compliance measures, including mandatory audits and risk assessments, while Important Entities experience comparatively relaxed oversight, focusing on post-incident evaluations.
- Both essential and important entities must comply with NIS 2 and all requirements apply the same way to both essential and important entities.



What Should I do?

Key Requirements

Governance and Risk Management
- Organizations must adopt comprehensive risk management practices, including cybersecurity strategies, governance, and regular assessments.
- There must be a clear assignment of cybersecurity responsibilities.
- Top management's action and accountability are mandatory requirements

Incident Reporting
- Mandatory and detailed reporting of security incidents with significant impact (within 24 hours of detection) to the national authority and any affected stakeholders.

Supply Chain Security
- Extended accountability not only for direct service providers but also for supply chain security.
- Companies must ensure their suppliers' cybersecurity practices align with NIS 2.

Member State Cooperation
- Member states must collaborate and share information regarding cybersecurity threats and incidents through their National CSIRTs.
- Establishing a network for rapid communication among member states is essential for effective response.

Business Obligations
- Businesses must ensure the security of their network and information systems against cyber threats.
- Businesses are responsible for implementing appropriate technical and organizational measures to safeguard data.

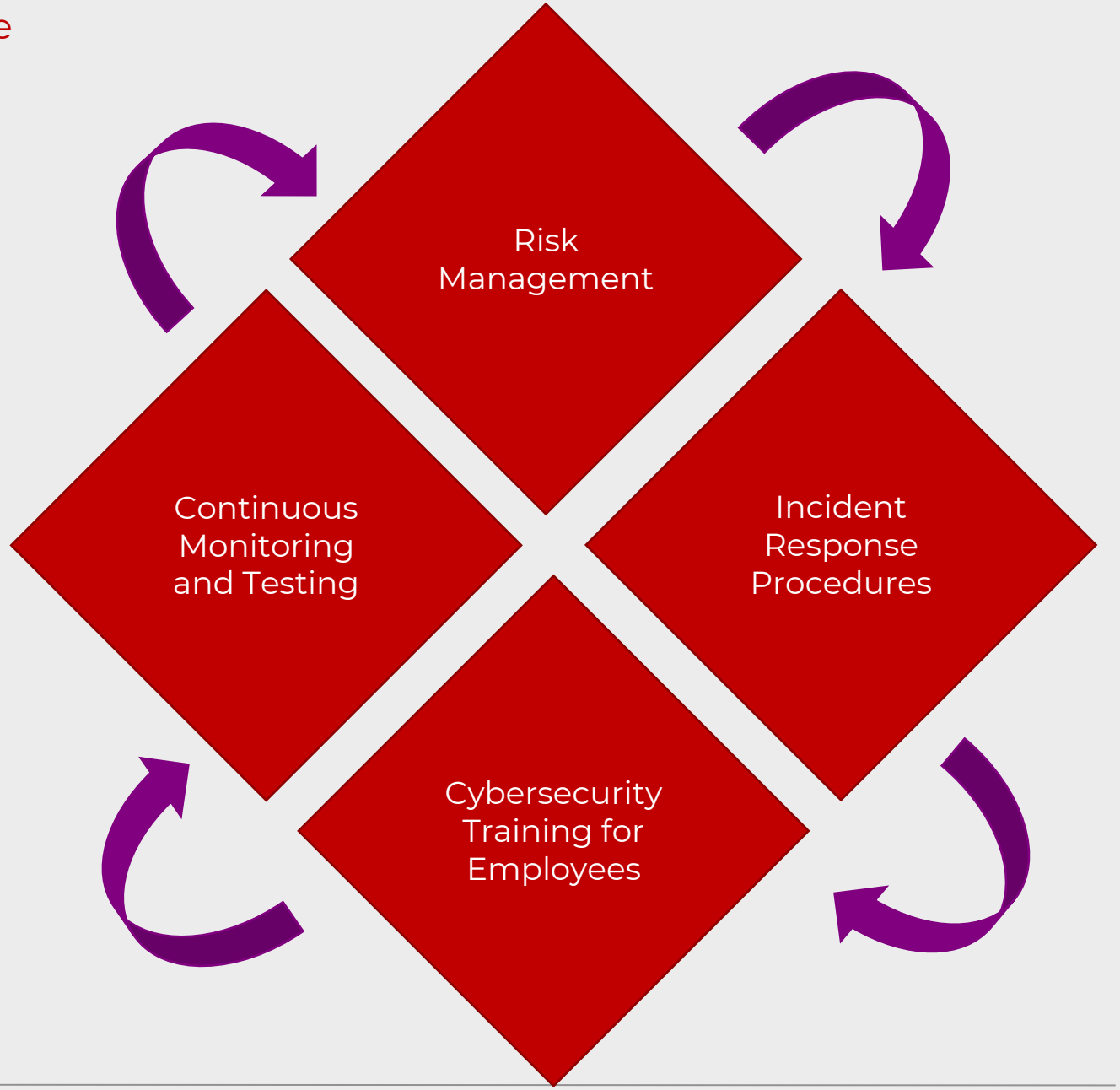
Compliance Requirements
- Organizations must comply with national cybersecurity strategies and frameworks established by member states.
- Regular audits and assessments will be necessary to ensure ongoing compliance with the NIS 2 Directive.

Compliance Checklist for Greek Businesses

- **Classification Awareness**: Businesses must accurately identify their classification as Essential or Important Entities to understand specific compliance obligations and associated cybersecurity measures.
- **Gap Analysis**: Identify gaps in compliance with the NIS 2 Directive.
- **Engagement with Authorities**: Active communication with regulatory bodies is crucial for receiving guidance and participating in initiatives that enhance compliance and cybersecurity practices.
- **Stay Updated**: Continuously monitor and adapt to changes in legislation and regulations.

Cybersecurity Best Practices for NIS 2 Compliance

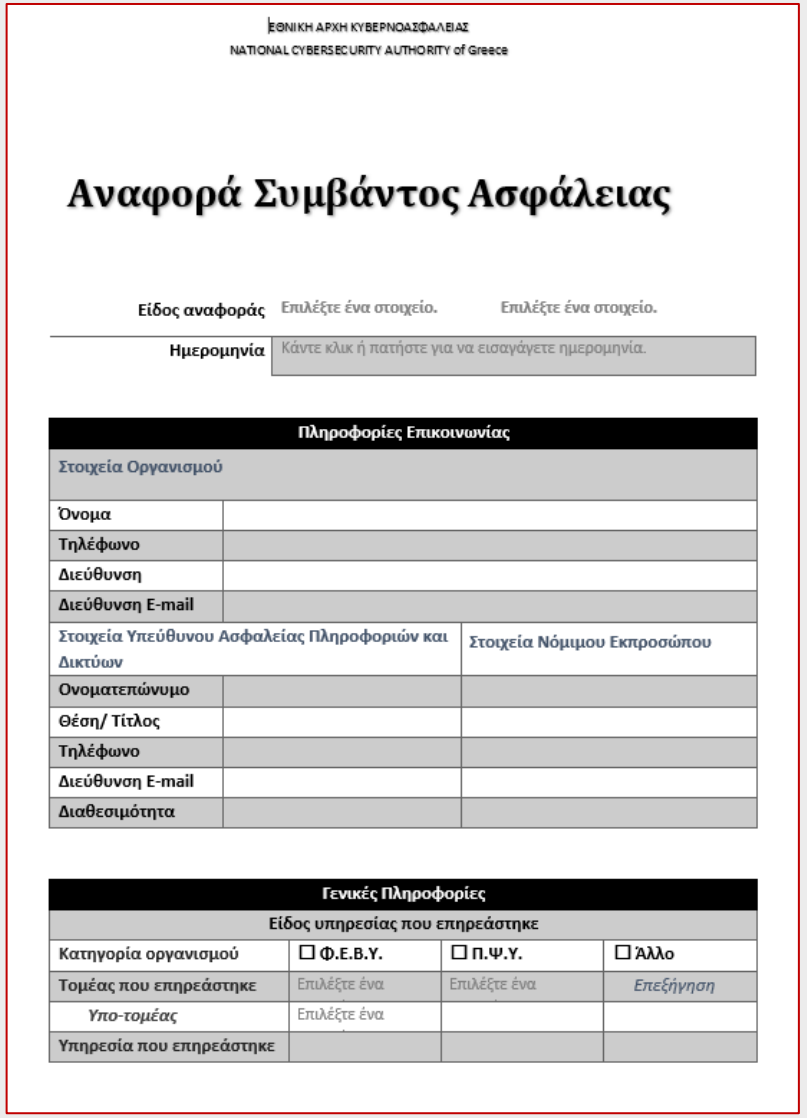
- Top Management Buy-In
- Gap Analysis
- Risk Assessment
- Security Governance
- Suppliers' Management
- Incident Management
- Business Continuity and Disaster Recovery.
- Real-time Monitoring
- Security Training and Awareness
- Internal Audits
- Continuous Improvement



Timely Incident Notification

Organizations(both essential and important) must report significant cybersecurity incidents to national CSIRTs within 24 hours of detection, followed by a detailed notification within 72 hours, ensuring rapid response and enhanced situational awareness across the EU.

Incidents may be reported using the available templates provided by the National Cyber Security Authority here: https://mindigital.gr/dioikisi/kyvernoasfaleia



ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
NATIONAL CYBERSECURITY AUTHORITY of Greece

Αναφορά Συμβάντος Ασφάλειας

Είδος αναφοράς Επιλέξτε ένα στοιχείο. Επιλέξτε ένα στοιχείο.

Ημερομηνία Κάντε κλικ ή πατήστε για να εισαγάγετε ημερομηνία.

Πληροφορίες Επικοινωνίας			
Στοιχεία Οργανισμού			
Όνομα			
Τηλέφωνο			
Διεύθυνση			
Διεύθυνση E-mail			
Στοιχεία Υπεύθυνου Ασφαλείας Πληροφοριών και Δικτύων		Στοιχεία Νόμιμου Εκπροσώπου	
Ονοματεπώνυμο			
Θέση/ Τίτλος			
Τηλέφωνο			
Διεύθυνση E-mail			
Διαθεσιμότητα			

Γενικές Πληροφορίες			
Είδος υπηρεσίας που επηρεάστηκε			
Κατηγορία οργανισμού	☐ Φ.Ε.Β.Υ.	☐ Π.Ψ.Υ.	☐ Άλλο
Τομέας που επηρεάστηκε	Επιλέξτε ένα	Επιλέξτε ένα	*Επεξήγηση*
Υπο-τομέας	Επιλέξτε ένα		
Υπηρεσία που επηρεάστηκε			

How NIS 2 Affects Supply Chain Management

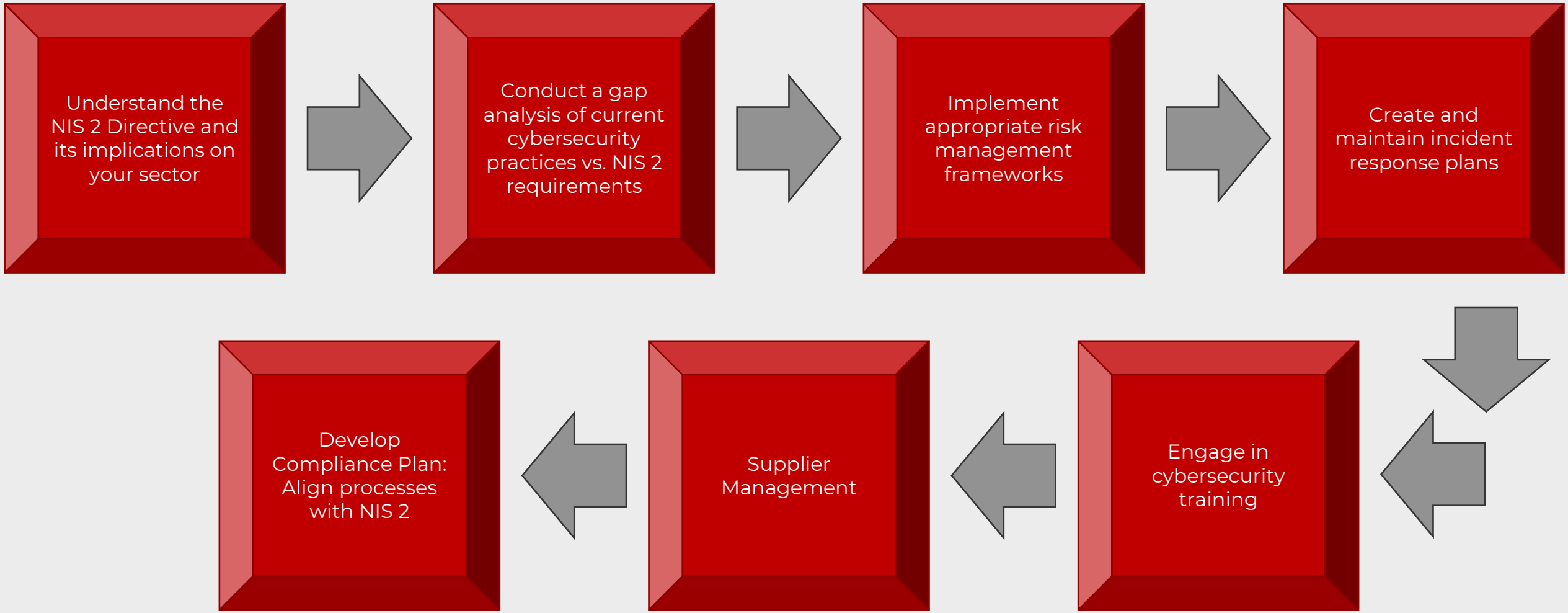
Which suppliers should comply?

- All entities which are considered to be in scope of NIS 2.
- Suppliers who are not considered to be in the NIS 2 scope may be influenced if they deliver services or products to an in-scope NIS 2 entity.

How to ensure suppliers' compliance?

- Suppliers that are not in scope of NIS 2 will not be supervised by the national authority, but they will need to be supervised by their clients.
- A Vendor Risk Management program should be in place to identify, evaluate and prioritize suppliers' risks.
- A supplier's Business Impact Analysis must be conducted to determine each supplier's criticality to a company's operations.
- Regular security audits and real-time monitoring of the supplier's compliance with security policies must be implemented.

Compliance Process for Greek Businesses



Collaborating with Authorities

Engage with the Hellenic Cybersecurity Authority for guidance.

+

Meet Compliance Requirements in coordination with national authorities.

Change of the landscape for Greek Businesses

- Adaptation costs for implementing necessary cybersecurity measures.
- Impact through supply chain provisions, despite being outside the direct scope.
- Medium-sized enterprises that are directly in the scope face disproportionate resource allocation challenges compared to larger organizations.
- Need to develop technical expertise within Greek organizations.
- Need to engage third-party cybersecurity companies and use their services.
- Keeping up with evolving cybersecurity threats and regulation updates.

Opportunities for Greek Businesses

- ✓ Potential to improve operational efficiency and customer trust through enhanced cybersecurity.
- ✓ Top management approval of cybersecurity countermeasures using the NIS 2 Directive.
- ✓ Ensure business continuity.
- ✓ Regulatory Compliance: Avoid penalties and legal consequences.

Tools and Resources for Compliance

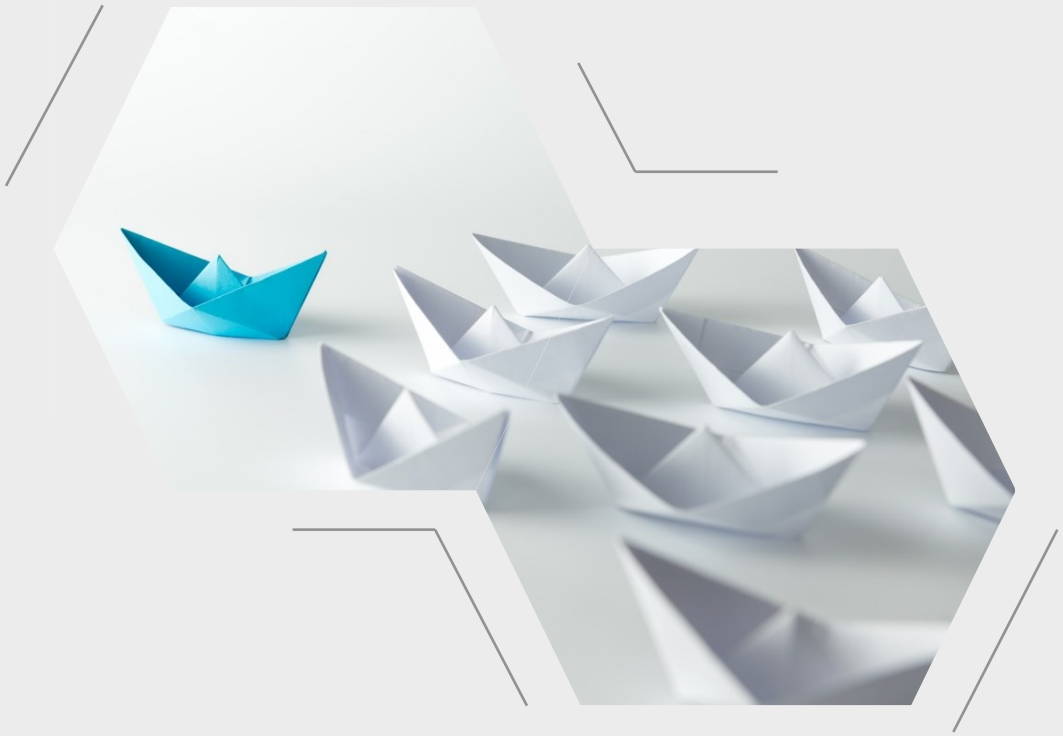
Compliance Software Tools: Automate reporting, tracking, and risk assessments.

External Consultants: Expert advice on meeting NIS 2 requirements.

Ongoing NIS 2 Ongoing Compliance

- Regular updates on new laws, regulations, and security threats.
- Combine NIS 2 with other regulations/standards like GDPR, DORA and ISO 27001.
- Create unified cybersecurity strategies for seamless compliance.
- Conduct regular internal and external audits for compliance.
- Perform at least 1 penetration test per year for assurance purposes.
- Evaluate effectiveness and implement improvements.

Conclusion



Summary of NIS 2 Impact:

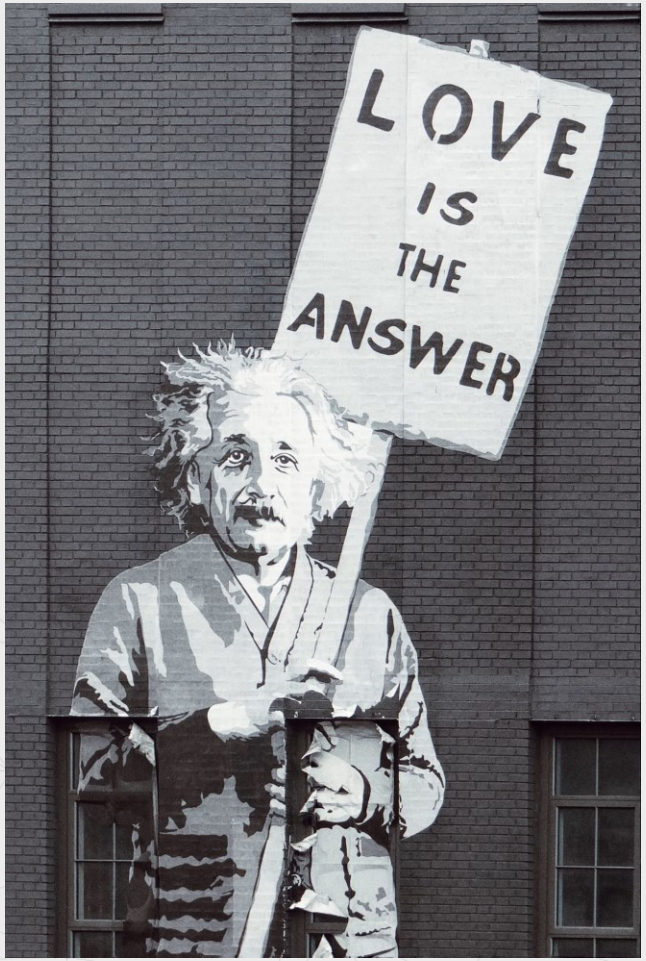
- NIS 2 significantly strengthens the cybersecurity posture of the EU and Greece.
- Greek businesses must prioritize cybersecurity and Incident Response processes to comply with NIS 2.
- By doing so, they not only mitigate risks but also contribute to the overall resilience of the EU's digital infrastructure.

Next Steps:

- Start the compliance process today to meet the upcoming deadlines.

We have to guard our (cyber) frontier!

Questions?



www.twelvesec.com
hello@twelvesec.com

Thank you!

Get in touch:

- Twitter
- Linkedin
- Facebook
- Github
- Instagram

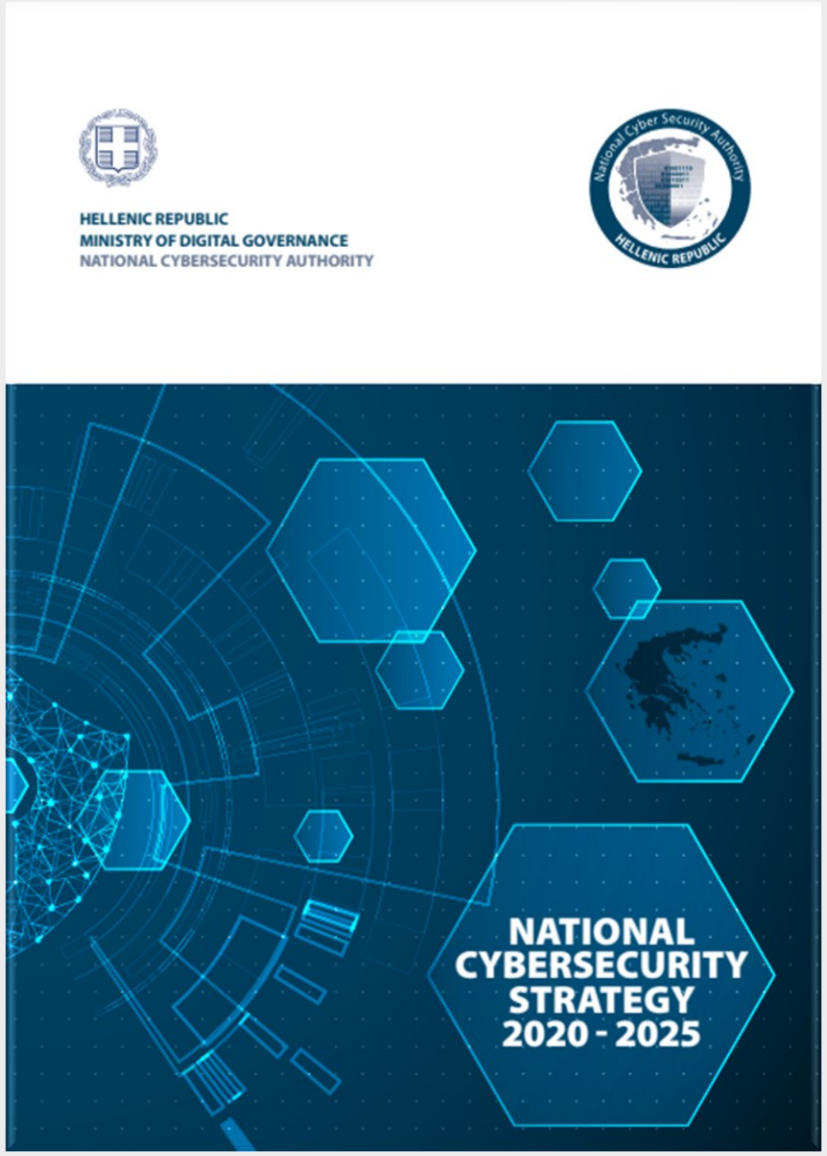
www.twelvesec.com
hello@twelvesec.com

Annex A – Additional Data

www.twelvesec.com
hello@twelvesec.com

National Cybersecurity Strategy

- The National Cybersecurity Strategy has been established on December of 2020, and it was last updated on December of 2023.
- It identifies key threats, threat agents and new technological challenges.
- The Gap Analysis performed recognized six (6) priorities: Contingency Planning, Incident Reporting, Security and Privacy Protection, Research and Development, Public-Private Partnerships (PPPs), Investments in Security Measures.
- Five (5) strategic goals were defined: cybersecurity governance, shielding critical infrastructure, incident management, research and development, awareness.



Completed Projects:

- Update of the National Cybersecurity Strategy and development of an action plan.
- Development of a manual-guide (handbook) of good cybersecurity practices.
- Formulation and implementation of an Operator Maturity Level Assessment Guide.
- Support actions to upgrade critical infrastructure security systems and capabilities.
- Operation of a platform to protect websites against cyber-attacks.
- Operation of a security assessment platform for the country's critical infrastructures and supervisory monitoring of Greek Cyberspace.
- Establishment of a real-time monitoring system for the availability of the websites of Governmental Organizations and critical infrastructures of the country.
- Vulnerability testing (Penetration Testing) of the websites and networks of the Governmental Organizations and critical infrastructures of the country.
- Development and maintenance of an Asset Registry of networks, hardware, devices, systems and information assets of the country's critical infrastructure.
- Conducting audits - inspections of the country's critical infrastructure.

Projects in Progress:

- Development of an integrated cybersecurity management framework.
- Conducting a risk assessment study at national level.
- Preparation of an Emergency Plan for dealing with cyber crises.
- Establishment of a sharing information platform for cybersecurity threats and incidents.
- Carrying out information and awareness-raising activities (seminars, workshops and seminars) on cybersecurity.
- Establishment of a platform and tools for vulnerability assessment & penetration testing.
- Design and institutionalization of a framework of controls - inspections of the country's critical infrastructure.
- Development of Cybersecurity R&D Agenda.
- Development of Cybersecurity Investment Toolkit

NIS 2 – Essential and Important Entities

Annex I: Sectors of high criticality

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: ***only*** if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
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	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: ***only*** if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(***only*** if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

NIS 2 – Important Entities

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
Annex II: other critical sectors				
POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
WASTE MANAGEMENT	(*only* if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
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)	IMPORTANT	IMPORTANT	NOT IN SCOPE
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and Article 28			

Annex B – References

www.twelvesec.com
hello@twelvesec.com

References

NIS 2 Directive - New rules on cybersecurity of network and information systems: https://digital-strategy.ec.europa.eu/en/policies/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): https://eur-lex.europa.eu/eli/dir/2022/2555

NIS 2 CSIRTS (Computer Security Incident Response Teams) Establishment: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network

NIS 2 EU CyCLONE (EU Cyber Crisis Liaison Organization Network) Establishment: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone

EU CER Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (definition of essential and important entities): https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

Incident Report Template by the Hellenic Cybersecurity Authority: https://mindigital.gr/wp-content/uploads/2020/01/Incident_Report.pdf

Deadline for self-registration of Greek companies: https://mindigital.gr/archives/7164

Greek Law 5160/2024 (transposition of NIS 2): https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=NIM:202405334

National Cybersecurity Strategy: https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf

Digital Transformation Bible: https://digitalstrategy.gov.gr/en/vivlos_pdf?page=210

Cybersecurity projects in place by the Hellenic Cybersecurity Authority: https://digitalstrategy.gov.gr/en/sector/diginf_cybersecurity

NIS 2 Essential and Important Entities: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf

NIS 2 Requirements: https://nis2directive.eu/nis2-requirements/

Who are affected by NIS 2: https://nis2directive.eu/who-are-affected-by-nis2/

NIS 2 Implementation-Challenges and priorities: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf