Cybersecurity legal and regulatory landscape

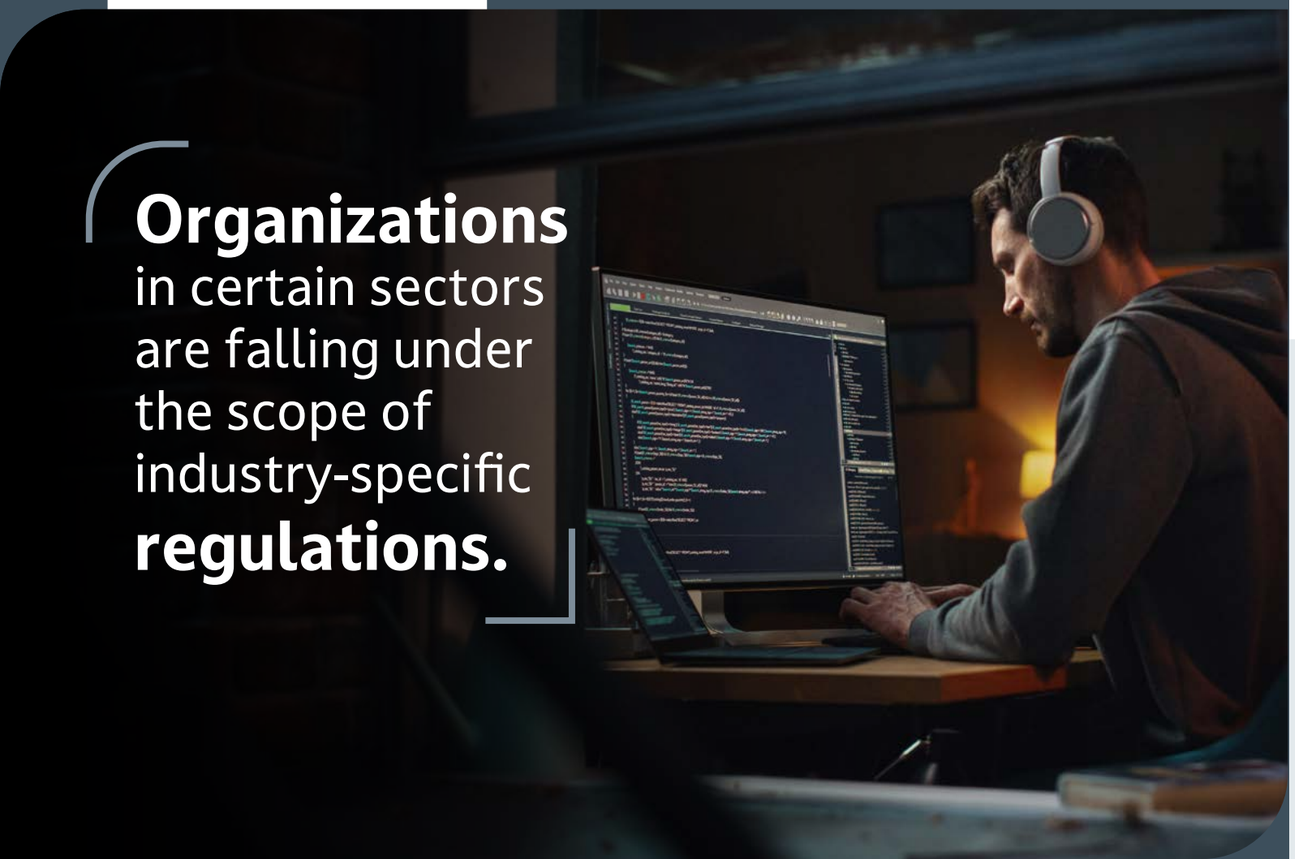
Challenges & opportunities

Building a better working world

Microsoft

Contents

1 Introduction



Organizations in certain sectors are falling under the scope of industry-specific **regulations.**

1.1. Purpose of the report

The significant challenges arising from the digitalization of organizations' operating environment as well as from a range of new emerging technologies have formed a dynamic and complex regulatory environment with organizations obliged to adhere to multiple compliance requirements at a national and regional level. Moreover, organizations in certain sectors are falling under the scope of industry-specific regulations. The regulatory changes, combined with an ever-shifting landscape in terms of relevant cyber risks, threats and actors, increase management complexity both for business and for cybersecurity teams, as areas of convergent of overlapping regulations must be identified. However, at the same time, this can introduce improvement opportunities for new growth areas.

In this context, this report aims to:

- Provide a holistic analysis of the current Cybersecurity legislative and regulatory landscape of the Greek and EU market.
- Identify the challenges that organizations face when trying to ensure compliance with the plethora of requirements.
- Highlight how Microsoft can support with addressing these challenges and allow organizations to gain competitive advantage and achieve operational excellence.

1.2. Scope of the report

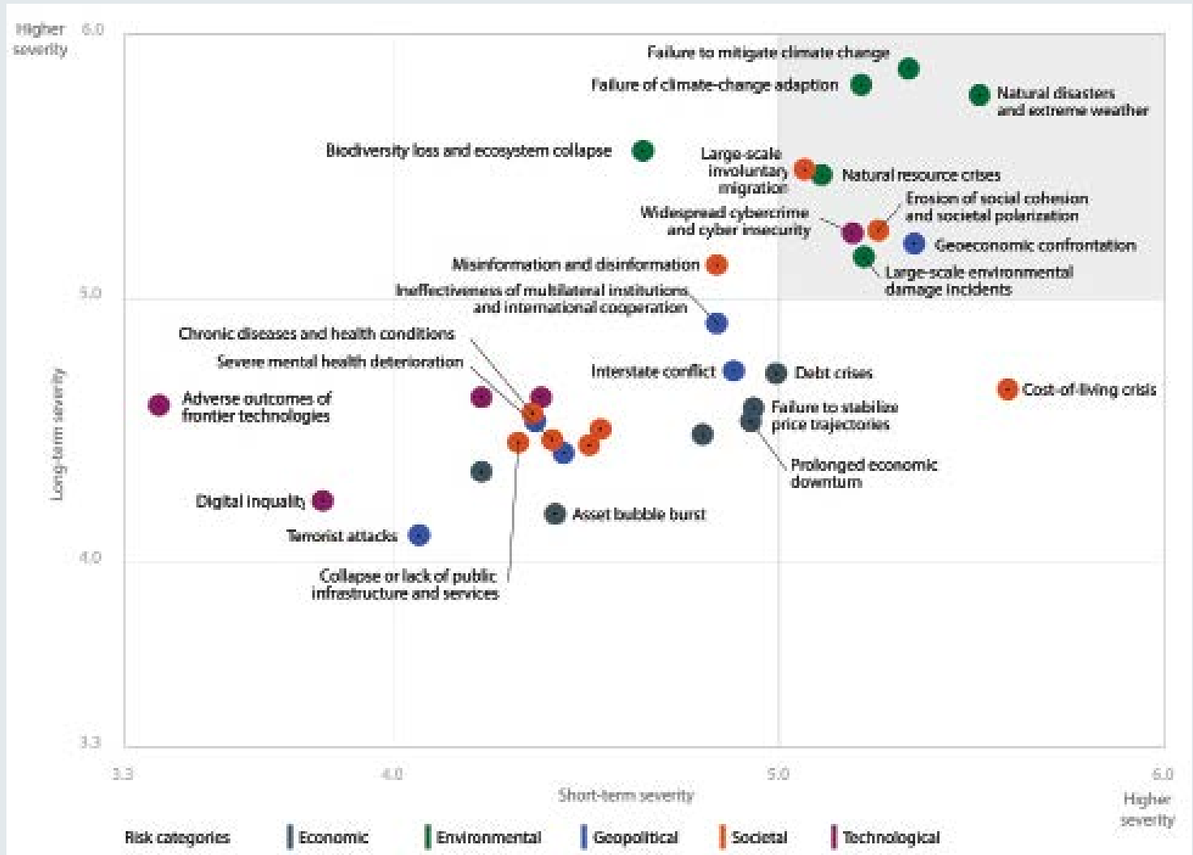
The scope of this report refers to the Cybersecurity laws and regulations that are currently in force and are applicable for organizations established in Greece as well as organizations which operate on a regional or global scale, i.e., laws enforced by Greek authorities such as the Ministry of Digital Governance, the Hellenic Telecommunications and Post Commission, the Hellenic Data Protection Authority, as well as the European Union.
Furthermore, in order to further expand on the subject matter and deep dive into the challenges organizations in Greece are facing, a survey encompassing various aspects of the issue at hand has been performed. The survey respondents include Cybersecurity and privacy professionals such as CISOs, Information Security Managers, Data Protection Officers, in organizations operating in Greece in various industries, such as Financial, Energy, Telecommunications and Public Sector.

2 Report background

Widespread cybercrime and cyber insecurity is a **top risk** over the next 10 years.

2.1. Cyber Threat Landscape Overview

The unchecked rate of digitalization, along with the rapid adoption of new technologies introduces vulnerabilities that threat actors, such as cyber criminals, nation-states or even insiders, can exploit for personal, ideological, economical, or geopolitical profit. Historically, cyber threats have been evolving in tandem with the relevant technological advancements. Early instances of “script kiddies”, who initiated attacks for amusement, experimentation or notoriety, have gradually given way to more sophisticated attackers, including malicious insiders, criminal networks and nation state-sponsored actors as well as, more recently, roboticized Artificial Intelligence and Machine Learning attacks.

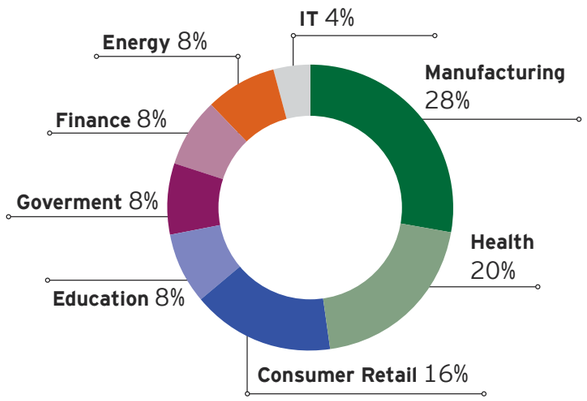


It is evident that Cybersecurity is now a main concern and is constantly present in Boards’ agendas, as the realization is dawning that every organization is at risk and the threat of a cyber-attack is more likely and daunting than ever. In fact, according to World Economic Forum’s Global Risk Report 2023 , cyber-attacks on critical infrastructure constitute one of the top five risks for 2023 with the greatest potential impact on a global scale, while widespread cybercrime and cyber insecurity is a top risk over the next 10 years, topped only by environmental and societal related risks (Figure 1).

Over the last few years cyber-attacks have grown exponentially, which was also the case for 2021-2022, both in terms of number and severity according to ENISA's latest Threat Landscape Report . Indicatively, the frequency of specific attacks such as ransomware and phishing has increased significantly, especially as a result of the shift to remote work, which was perceived as a major opportunity by attackers aiming to capitalize on the changing work environment.

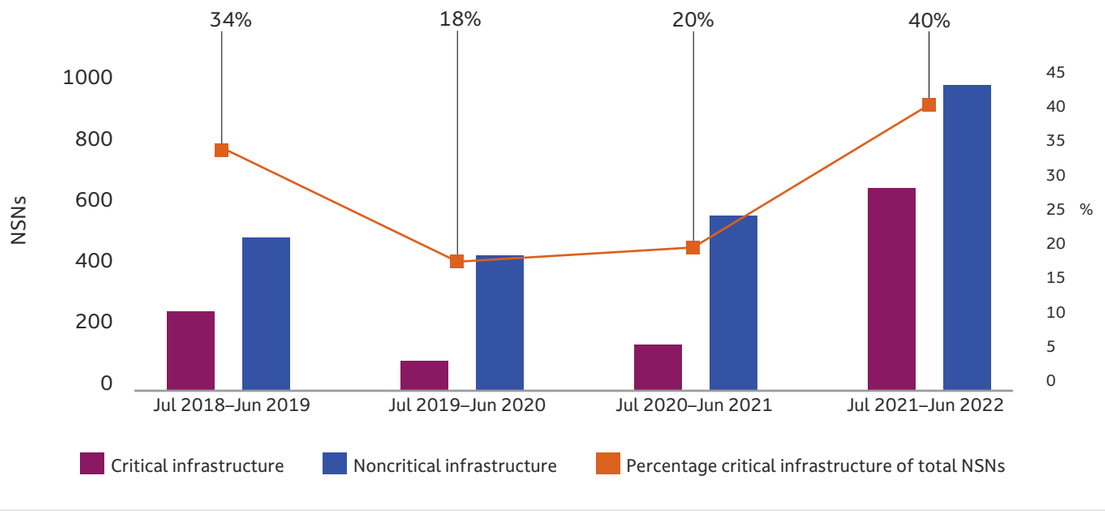
More specifically, according to IBM's Cost of a Data Breach 2022 Report , last year showed a significant increase in breaches caused by ransomware attacks, growing 41% compared to 2021. Breaches caused by phishing campaigns also grew by 48%, constituting the most common vector for initial access according to ENISA's latest Threat Landscape Report, while it is noted that 40% of all cyber threats now take place directly through the supply chain.

Furthermore, according to Microsoft's Digital Defense Report 2022 , approximately 710 million phishing emails are blocked weekly by relevant Microsoft security solutions, while a steady growth of ransomware attacks is observed since 2019. The latest findings (Figure 2) show that the most targeted sectors are Manufacturing (28%) and Health (20%) followed by Consumer retail companies (16%).



Additionally, following the invasion of Ukraine by Russia, the number of cyber-attacks stemming from nation state groups against both critical and non-critical infrastructure has risen significantly. According to Microsoft's Threat Intelligence: A year of Russian hybrid warfare in Ukraine Report , the main trends which can be identified since Russia's invasion include an increase in the use of ransomware as a deniable destructive weapon, the utilization of diverse toolkits to gain initial access to targets, and an increased use of hacktivists for power projection. More broadly, the aforementioned Digital Defense Report, 40% of all nation state notifications (NSNs) targeted critical infrastructure, with threat actors focusing on companies in the IT sector, financial services, transportation systems and communications infrastructure.

Critical infrastructure trends



Finally, as affirmed by the same Report, the concept of Cybercrime as a Service (CaaS) is a growing and evolving threat worldwide with Phishing as a Service (PhaaS) being a prime example of an end-to-end cybercrime service offered by cybercriminal merchants on a subscription basis. The main threat posed by PhaaS is related to its accessibility, as it can, in theory, be used by any interested party by selecting a phishing site template or design among the hundreds offered, providing an e-mail address to receive credentials obtained from phishing victims and finally paying the PhaaS merchant in cryptocurrency.

2.2 Rapid technology advancements as a key factor to the evolving cyber threat landscape

The latest key technology advancements, as a result of the aforementioned rapid digitalization, can be identified across Cloud Computing, OT-IoT, Blockchain, Artificial Intelligence and Machine Learning.

Cloud Computing

An important factor in the overall digitalization of all industries, especially in a post-pandemic world where the work-from-home model is increasingly adopted by organizations across all sectors, is the accelerated implementation and growth of cloud computing solutions. The move to such solutions is key in supporting increasingly complex organizational requirements and objectives, enhancing their speed to market, agility and overall responsiveness. However, the migration to cloud-based solutions requires a shift in the overall security paradigm, as organizations need to consider cloud strategies which can properly enable their business and address the relevant security concerns at the same time.

As a result of this, the main challenge faced by organizations is obtaining a clearer view and overall understanding of cloud operations, the available service models (SaaS, PaaS and IaaS) as well as the security requirements they entail. For instance, the introduction of the shared responsibility model, through which providers must ensure that their infrastructure and their clients' data are adequately secured, while the clients themselves must in turn make sure that strong access and authentication controls are implemented, requires the organizations to define, implement and adapt their cloud strategies accordingly which, as stated, requires a deeper understanding of the relevant security requirements.

OT / IoT

Operational Technology (OT) refers to the monitoring and operation of industrial devices, processes and overall infrastructure, through the use of the relevant hardware and software assets. OT and IT technologies are rapidly converging, handling remote as well as data recovery operations, and thus leading to new attack vectors and an overall expanded attack surface. Additionally, and due to their focus on Industrial Control Systems (ICS), attacks on OT infrastructure differ from traditional attacks against IT environments, potentially having tangible consequences in the real world, and even leading to posing an actual threat of serious injury or loss of life, as a result of component failure.

At the same time, Internet of Things (IoT) devices, which include printers, security cameras and physical access controls, are rapidly being adopted by organizations in both industrial as well as non-industrial sectors, as they are critical in more efficiently supporting day-to-day operations. Similarly to OT however, IoT devices may act as additional attack conduits, greatly expanding the organizational attack surface, especially through the exploitation of unmanaged devices, and potentially leading to severe data loss. More specifically, exposed IoT devices are especially susceptible to malware attacks (e.g. using Mirai), including by threat actors running malware as a service operations, as well as unauthorized remote access through unsecured ports discoverable through the internet, exploitation of vulnerabilities and web-based exploits over HTTP.

Thus, in order to ensure adequate security for both the OT and IoT ecosystems, organizations must define and implement an appropriate roadmap, taking into consideration that the relevant assets must be identified, a deeper understanding of the vulnerability ecosystem must be acquired, existing security mechanisms must be leveraged, an OT and IoT governance system must be defined, and appropriate security mechanisms must be implemented in accordance with the relevant requirements.

Blockchain

The Blockchain is an emerging technology with up-and-coming applications in industries such as the utilities and the energy sector, as well as the technology sector at large, as it solves a number of ownership-related issues. Blockchain technologies are still in their infancy stages and have brought about new security challenges to be tackled.

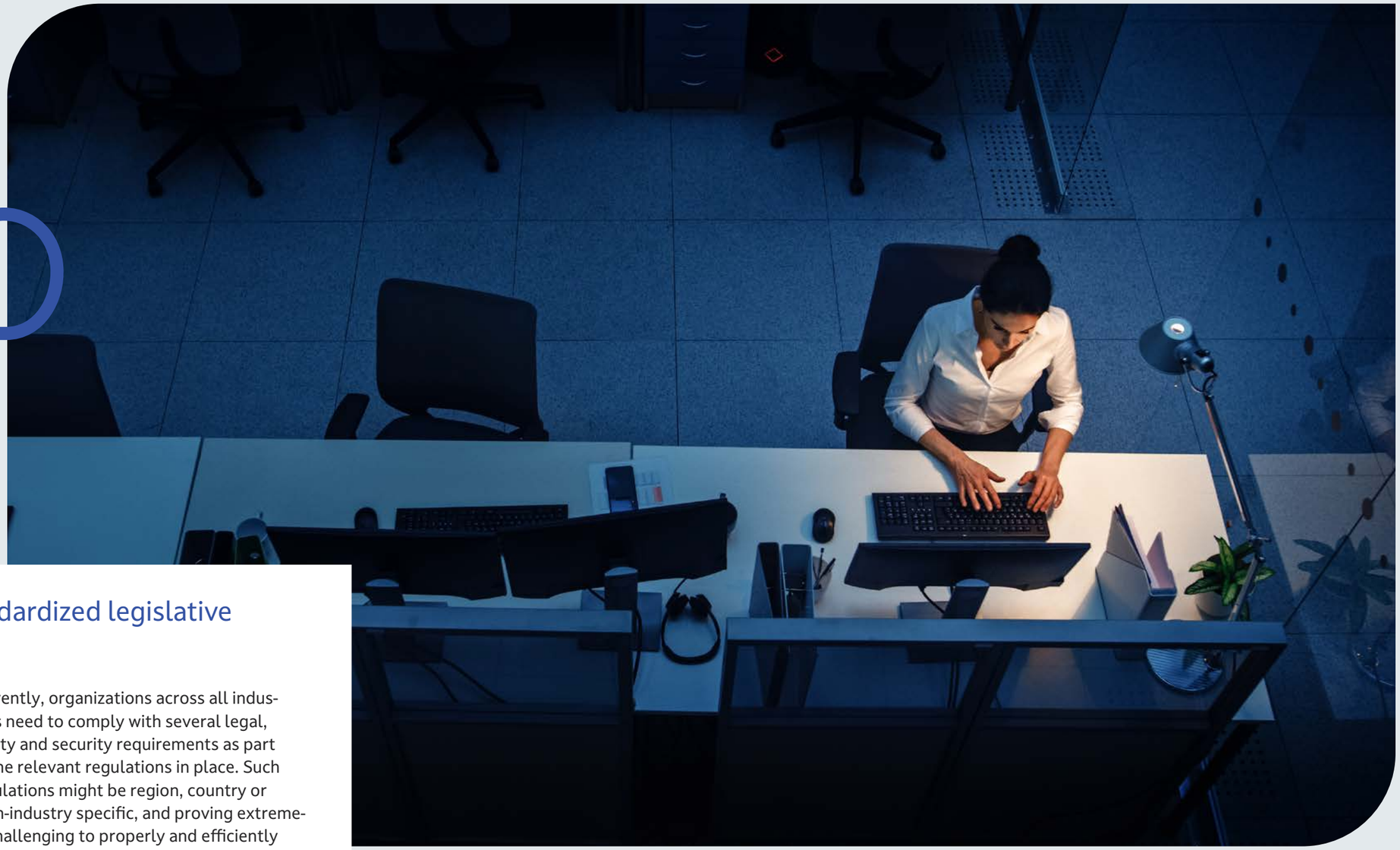
Although Blockchain technologies have specific security qualities, as they are inherently based on cryptographic, decentralization and consensus principles, also depending on the implementation of these technologies (permissioned/private or permissionless/public), known infrastructure vulnerabilities can be manipulated and exploited by malicious actors.

More specifically, Blockchain technologies are susceptible to prevalent types of attacks such as phishing, as well as more sophisticated attack types such as routing and Sybil attacks , thus requiring effective wallet/key management, smart contract vulnerability management and proper phishing controls in place.

Artificial Intelligence / Machine Learning

Finally, Artificial Intelligence (AI) and Machine Learning (ML) capabilities and solutions are increasingly being utilized across a variety of applications, including being leveraged as part of AI-based tools for threat detection, vulnerability management, overall monitoring and, ultimately, response. Conversely, such solutions are also potentially vulnerable to direct data manipulation attacks exploiting the implemented algorithms altering their functionality. More critically, however, AI and ML capabilities are also being used in cyber-attacks, as they become more sophisticated and complex, more effectively navigating, identifying and exploiting potential vulnerabilities[8].

[8] *AI and ML capabilities are now used in Advanced Persistent Threats (APTs), phishing and Distributed Denial of Service (DDoS) attacks.*



2.3 The need to establish a standardized legislative and regulatory landscape

The aforementioned technology advances have dictated the need for proper regulatory and legislative controls. However, this has led to a rapidly increasing number of relevant requirements, further fragmenting the overall legislative and regulatory landscape as a whole.

This high degree of fragmentation also poses a significant cyber security challenge, as the landscape is expected to become even more fragmented going forward and thus, more time consuming for companies as well as the relevant stakeholders to manage.

Currently, organizations across all industries need to comply with several legal, safety and security requirements as part of the relevant regulations in place. Such regulations might be region, country or even-industry specific, and proving extremely challenging to properly and efficiently map. To that end, and specifically at the legislative-regulatory level, effort should be made to standardize the overall landscape to the highest possible degree, while ensuring that appropriate guidance is given to the affected organizations so that they are more aware of their obligations and the relevant requirements that they need to adhere to.

Regulations such as **region, country or even-industry specific,** are proving extremely challenging to properly and efficiently map.

3 Current state of play

The cybersecurity of the public and private sectors in the internal market has been set out as a **priority for the European Union**

3.1 Executive Summary

The cybersecurity of the public and private sectors in the internal market has been set out as a priority for the European Union in its strategic goal to become global leader in the digital era.

In this context, several policy initiatives and legislative acts have been adopted by the institutions of the EU. The timeline of the development of EU cybersecurity regulation is exhibited as follows:

EU cybersecurity regulations timeline

July 2016
Adoption of the NIS Directive

July 2019
Adoption and Application of the Cybersecurity Act

December 2020
European Cybersecurity Certification Scheme for Cloud Services

December 2020
Adoption of the EC Cybersecurity Strategy

September 2022
Proposal of the Cyber Resilience Act

December 2022
Adoption of the Digital Operational Resilience Act

January 2023
Adoption of the NIS 2 and the CER Directives

October 2024
Application of the NIS 2 Directive

January 2025
Application of the Digital Operational Resilience Act

January 2026
Application of the CER Directive

In line with the developments at EU level, Greece has adopted its National Cybersecurity Strategy 2020 – 2025 and has taken active steps towards upgrading the level of information security in the country. The main legislative acts on cybersecurity applicable in Greece are the following:

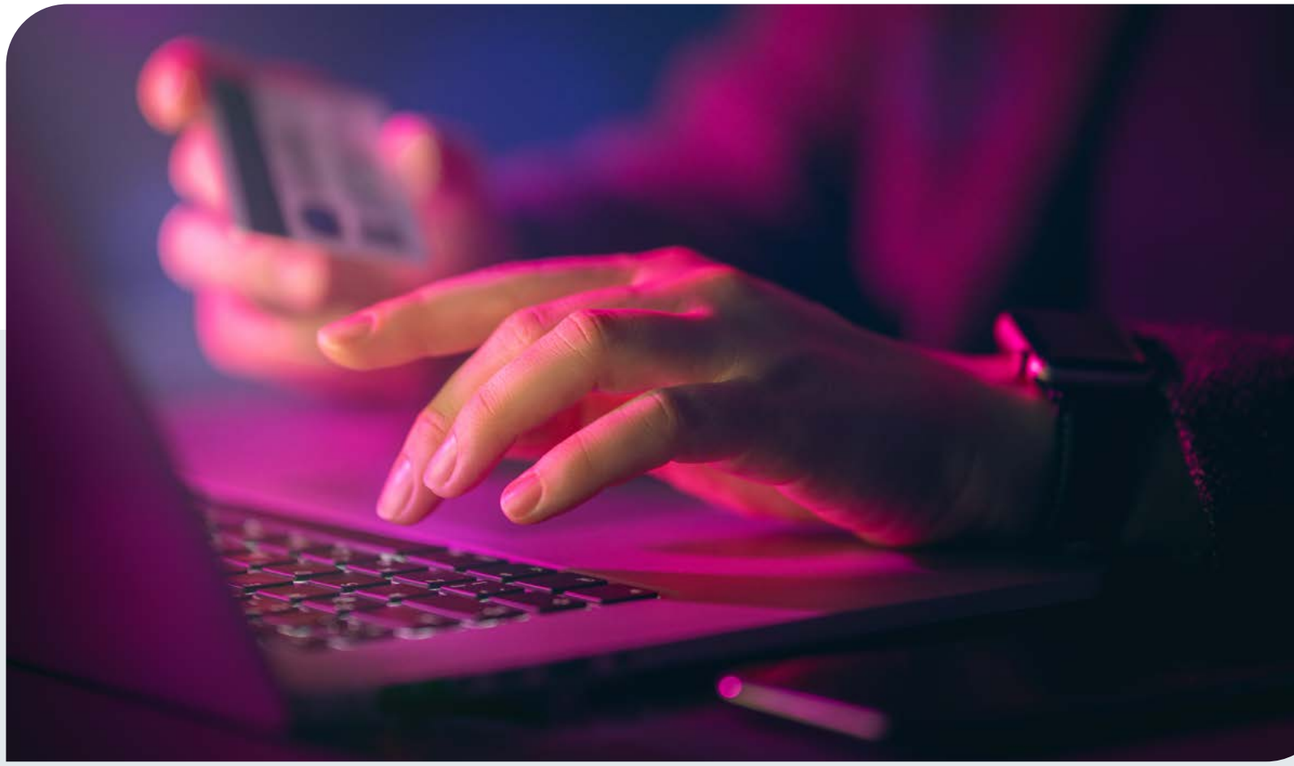
Main legislative acts on cybersecurity applicable in Greece

Act / Legislation	Description	Scope	Next Steps
Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector ("DORA")	Introduction of an advanced set of cybersecurity obligations for financial entities	• Credit and financial institutions • Crypto-asset service providers • ICT third-party service providers	• Entry into force on 27 December 2022 • Application from 17 January 2025
Greek Cybersecurity Framework Law 4577/2018 & Ministerial Decision 1027/2019	Crypto-asset service providers	• Operators of essential services • Providers of digital services	Publication of National List of Obligated Entities
Articles 109-223 of Law 4727/2020 the European Electronic Communications Code	ICT third-party service providers	Electronic communication network and / or service providers	Initiatives for the secure deployment of 5G networks according to the requirements of the EU 5G Toolbox
Articles 32-42 of Law 4961/2022	Application from 17 January 2025	Manufacturers, importers, distributors and operators of IoT devices	Adoption of Ministerial Decisions on the technical specifications and safety measures of IoT technology devices

In the past two years, significant developments have taken place at EU level in respect of cybersecurity legislation. In line with the EC Cybersecurity Strategy, the EU has adopted the NIS2 and CER Directives and the European Commission has proposed the Cyber Resilience Act. The transposition of the foregoing Directive into Greek law and the adoption of the Act will significantly change the regulatory landscape for cybersecurity in the country. The main points of the forthcoming developments on cybersecurity legislation are the following:

Main points of the Cyber Resilience Act, NIS II Directive and CERD

Act / Legislation	Description	Scope	Next Steps
Cyber Resilience Act	Enactment of horizontal cybersecurity requirements for hardware and software products with digital elements	• Manufacturers • Authorised representatives • Importers • Distributors of products with digital elements	Economic operators will have two years from entry into force to adapt to the requirements of the Act
European Cybersecurity Certification Scheme for Cloud Services	The European Cybersecurity Certification Scheme for Cloud Services looks into the certification of the cybersecurity of cloud services as a specific category of ICT services, allowing industries or verticals to adopt a security profile mechanism that is included in the scheme.	• Cloud Service Providers (CSPs) who wish to assess the security of their cloud services through third-party certification, • Cloud Service Customers (CSCs) who wish to benefit from the evidence provided with certified cloud services	The European Certification Scheme for Cloud Services was drafted and delivered in 2020 with the support of an Ad-Hoc Working group and the support of Member States. The text should now enter the process of the European Cybersecurity Certification Group for opinion.



Act / Legislation	Description	Scope	Next Steps
NIS II Directive	Expansion of the material scope of cybersecurity obligations to new categories of entities	• Entities within CERD scope • Electronic communications network or service providers • Trust service providers • Top-level domain name registries and domain name system service providers • Public bodies	• Entry into force on 16 January 2023 • Deadline to transpose by 17 October 2024 • Establishment of list of obligated entities falling by 17 April 2025
Critical Entities Resilience Directive (“CERD”)	Enactment of obligations for critical entities for the prevention, protection, resistance, mitigation, and recovery from incidents that have the potential to disrupt the provision of essential services.	Operators of essential services in sectors such as energy, transport, banking, financial market infrastructure, health, drinking water.	• Entry in force on 16 January 2023 • Deadline to transpose by 17 January 2026 • Establishment of national lists of critical entities by 17 July 2026

Taking into account the significant developments in the regulation of cybersecurity requirements at the EU and national level, Greek businesses which fall within the scope of relevant obligations will be required to establish adequate information security frameworks and execute respective compliance exercises, so as to be in line with the law.

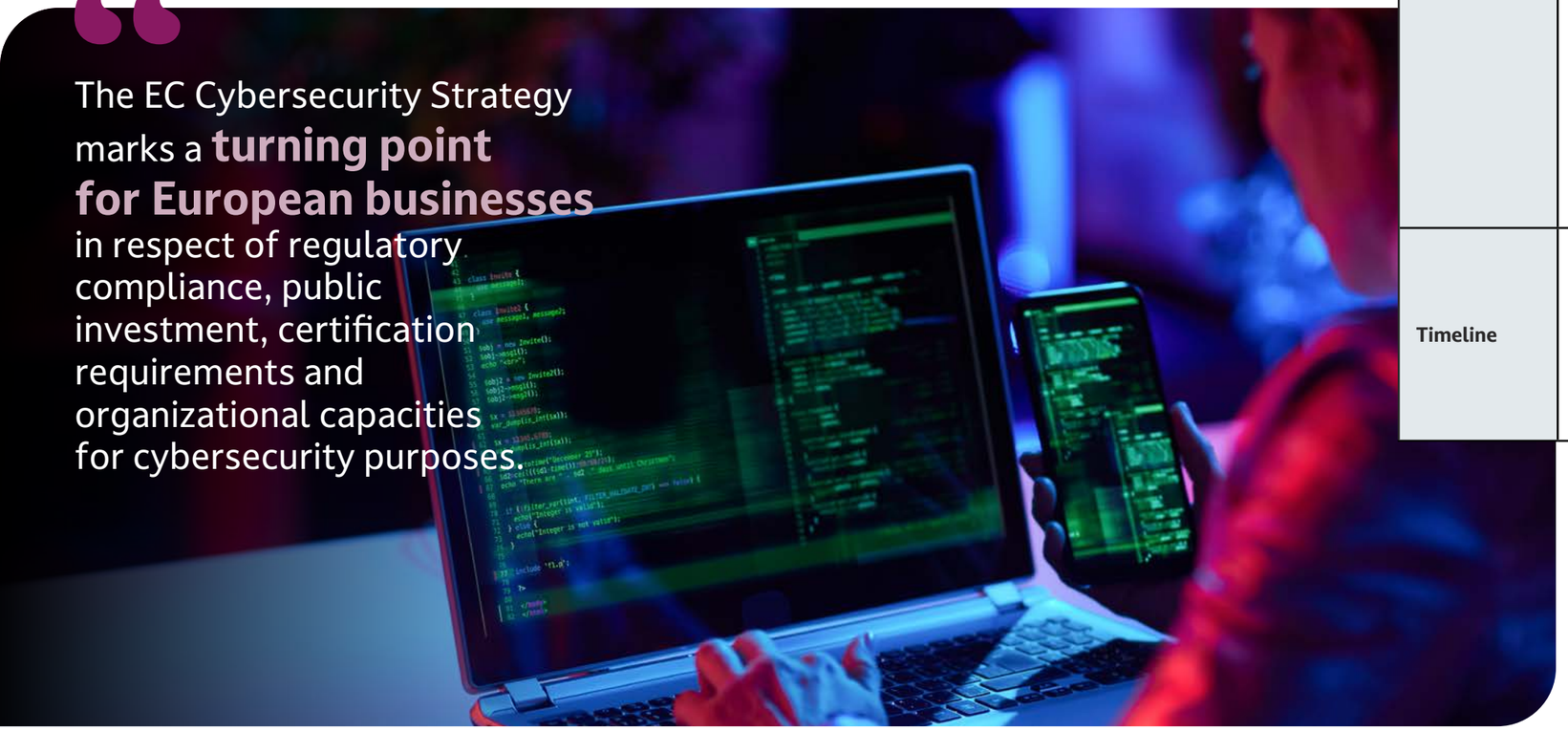
3.2 Policies

At the level of policy – making, the European Union has taken significant steps to boost the advancement of cybersecurity as strategic component in its plan for the digital transformation of businesses and ensure a fair and competitive digital economy of the continent.

Already back in 2019, the then newly appointed European Commission of Ursula von Der Leyen set out cybersecurity as a priority area for further action as part of its new digital strategy for a Europe fit for the Digital Age.

With its Cybersecurity Strategy[9], adopted on 16 December 2020, the European Commission aims to bolster the Union's collective resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies, by deploying regulatory, investment and policy instruments in three areas of action, i.e. (1) resilience, technological sovereignty and leadership, (2) building of operational capacity to prevent, deter and respond, and (3) advancement of a global and open cyberspace.

> The EC Cybersecurity Strategy marks a **turning point for European businesses** in respect of regulatory compliance, public investment, certification requirements and organizational capacities for cybersecurity purposes.



Focus Area	The EC Cybersecurity Strategy
Aim	• Resilience, technological sovereignty and leadership • Building operational capacity to prevent, deter and respond • Advancing a global and open cyberspace through increased cooperation
Key Actions	**Regulatory Actions:** • NIS 2 Directive • Cyber Resilience Act for an Internet of Secure Things • Critical Entities Resilience (CER) Directive **Investment Actions:** • European Cyber Shield • Secure quantum communication infrastructure (QCI) • Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres • European Digital Innovation Hubs **Policy Actions:** • Contingency plan for greater global internet security • Completion of the implementation of the EU 5G Toolbox • Joint Cyber Unit at EU level • Action plan to improve digital capacity for law enforcement agencies • EU Cyber Diplomacy Toolbox • EU External Cyber Capacity Building Agenda • Support of international standardization processes
Timeline	• Increased public investment for cybersecurity through the Digital Europe Programme, Horizon Europe and Recovery Plan for Europe. • Pan-European network of Security Operations Centres • Compliance with the NIS 2 Directive, Critical Entities Resilience Directive and Cyber Resilience Act.

In its consolidated Digital Compass strategy , adopted in 2021[10], the Commission further laid down its vision for the European way to a digitalized economy and society based on solidarity, prosperity, and sustainability, anchored in empowerment of its citizens and businesses, and ensuring the security and resilience of its digital ecosystem and supply chains.

[9] *European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, Brussels, 16.12.2020, JOIN(2020) 18 final, available: https://ec.europa.eu/newsroom/dae/redirection/document/72164.*

[10] *Commission Communication, 2030 Digital Compass: the European way for the Digital Decade, Brussels, 9.3.2021, COM(2021) 118 final, available: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf.*

Following the establishment of the Hellenic Cyber Security Authority, the Greek Ministry of Digital Governance adopted the Hellenic National Cybersecurity Strategy 2020 – 2025[11], envisioning a modern and secure digital environment of information and network infrastructures, applications and services in the country for the benefit of economic and social prosperity.

The Strategy lays down the following five strategic goals accompanied with specific initiatives for their implementation: (i) a functional cybersecurity governance system; (ii) shielding Critical Infrastructures and securing new technologies; (iii) incident management optimisation, fight against cybercrime and privacy protection; (iv) a modern environment for cybersecurity investments with emphasis on the promotion of Research and Development; and (v) capacity building, promoting information and awareness raising.

> The National Strategy provides a **clear action plan** for the Greek Cybersecurity Authority and highlights the gradual advancement in **the capacity of Greek public institutions to implement coherent policies** in the field of cybersecurity governance, impose regulation and exercise supervision on the private sector.

Focus Area	The Hellenic Cybersecurity Strategy
Aim	Establishment of a modern and secure digital environment of information and network infrastructures, applications and services in Greece
Key Actions	• Optimize organisational structures and procedures • Apply vigorous risk assessment and effective contingency planning • Strengthen national, European, and international collaborations • Comprehend technological developments and their effects on digital governance • Upgrade critical infrastructures' protection • Consolidate systems and applications by implementing enhanced security requirements • Optimise methods, techniques and tools utilised in incident analysis, response and reporting • Strengthen deterrence mechanisms and enhance operational cooperation • Cybersecurity for the protection of privacy • Encourage R&D initiatives • Provide investment incentives • Utilise PPPs • Building capacity by organising cybersecurity exercising activities • Apply state - of - the - art educational and training methods and tools • Promote open - ended cybersecurity information and awareness raising for Entities and citizens
Timeline	• Development of national cyber-threat registry, risk assessment and contingency planning • Implementation of an integrated cybersecurity framework for 5G networks • Implementation of a framework of security measures and actions for the Internet of Things (IoT) • Issuance of special security requirements for public ICT projects • Definition of requirements for providers of cybersecurity services

[11] *Ministerial Decision no. 34368/07-12-2020, Adoption of the National Cybersecurity Strategy 2020 – 2025, available: https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf.*

3.3 Legislation

In line with the EC Cybersecurity Strategy, the European Union has already adopted the Cybersecurity Act and the sectoral Digital Operational Resilience Act ("DORA") for the financial sector, which are directly applicable in Greece. In addition, the enactment of the Greek framework law 4577/2018 on cybersecurity lays down the basic cybersecurity requirements for essential service operators and digital service providers in the country.

With the aim to achieve a high level of cybersecurity, cyber resilience and trust within the Union, the Cybersecurity Act[12] strengthens the EU Agency for Cybersecurity ("ENISA") and introduces a framework for the establishment of European cybersecurity certification schemes for ICT products, processes and services.

Furthermore, articles 15-27 of Law 4961/2022 lay down the national rules complementing the Cybersecurity Act, in particular the designation of the National Cybersecurity Authority as national cybersecurity certification authority and the provision of its powers.

"By virtue of the Cybersecurity Act businesses shall be able to acquire **tailored and risk-based cybersecurity certification** for their ICT products, processes and services, which will be recognised across the European Union.

Focus Area	Cybersecurity Act
Scope	• Establishment of European cybersecurity certification schemes to attest that ICT products, ICT services and ICT processes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of data or functions or services.
Key Points	• Strengthened mandate for ENISA, which includes capacity-building, cooperation at EU level and Market, cybersecurity certification, and standardization • Rules for the establishment of an EU Cybersecurity Certification Framework and the process for the preparation, adoption and review of European cybersecurity certification schemes-before ENISA and the Commission • Rules for the designation of national cybersecurity certification authorities and the accreditation of conformity assessment bodies
Enforcement	• Member States shall lay down the rules on effective, proportionate and dissuasive penalties applicable to infringements of European cybersecurity certification schemes
Timeline	• The Cybersecurity Act has entered into force on 7 July 2019

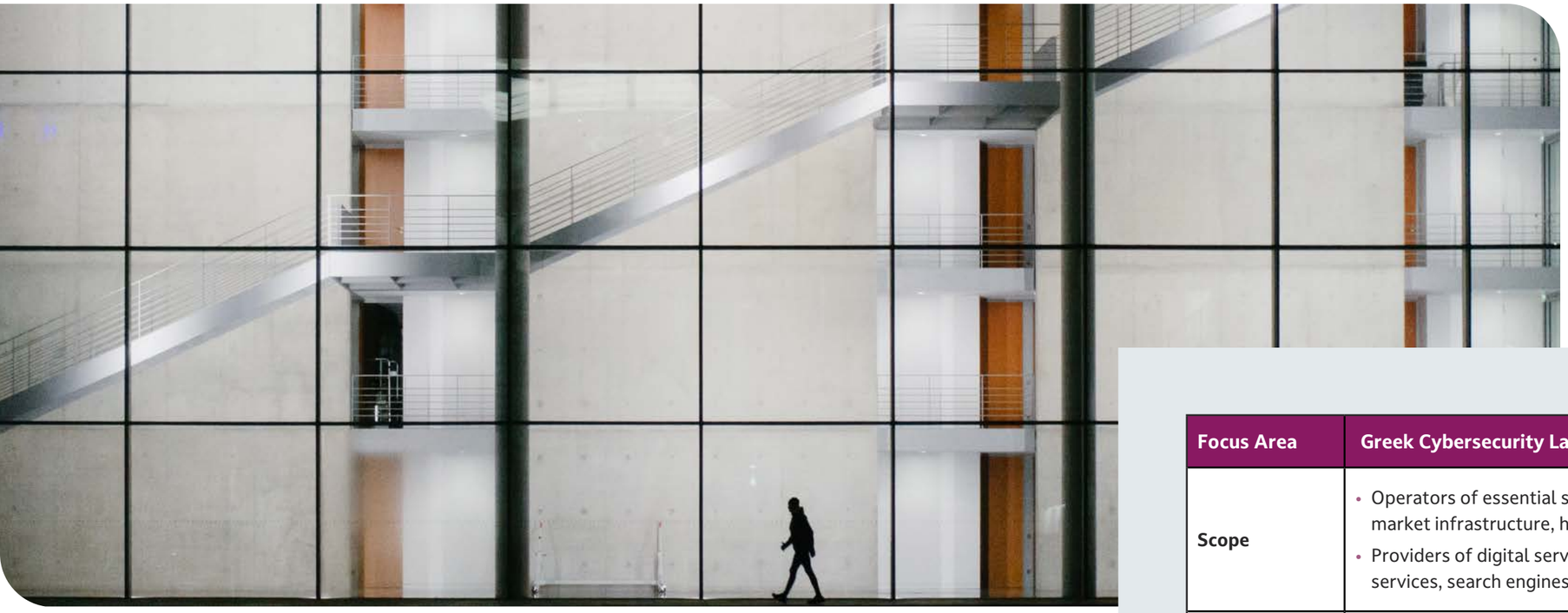
[12] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151, 7.6.2019, p. 15–69, available: https://eur-lex.europa.eu/eli/reg/2019/881/oj.*

Under article 48.2 of the Cybersecurity Act[13], there is a provision of such an establishment of a European cybersecurity certification scheme for cloud services. So far, the competent authority ENISA has not made any formal publication, except for a preparatory legal text, from which no rights can be derived and does not represent state of the art. The EUCS scheme intends to be applied to all cloud services following specific criteria, providing three levels of assurance. The criteria that must be meet are a) the design by default and the implementation of the cloud service b) the essential processes that must be followed for the development, deployment and operation of the cloud scheme. The EUCS scheme is a technical tool designed to provide information to costumers and to allow them to make informed decisions aiming at improving the Internal Market conditions and enhancing the level of security of cloud services, capabilities defined as application, infrastructure and platform.

Focus Area	European Cybersecurity certification scheme for cloud services
Scope	The European Cybersecurity Certification Scheme for Cloud Services looks into the certification of the cybersecurity of cloud services as a specific category of ICT services, allowing industries or verticals to adopt a security profile mechanism that is included in the scheme. The main aim consists in the improvement of the Internal Market conditions and the enhancement of the level of security of cloud services and their implementing capabilities. Users of the scheme may be cloud service providers (CSPs) who wish to assess the security of their cloud services through third-party certification, cloud service customers (CSCs) who wish to benefit from the evidence provided with certified cloud services to make informed decisions related to the security of these cloud services, regulatory authorities who wish to include security and assurance requirements on cloud services within their regulations and directives.
Key requirements	The EUCS scheme defines rules and mechanisms that may be combined to allow users to reach these objectives: • three assurance levels corresponding to levels 'basic', 'substantial' and 'high' as defined in the EUCSA • a set of security objectives and requirements defining objectives to be met by cloud s ervice providers for all certified cloud services, decomposed into requirements mapped to the assurance levels referred to above • an assessment meta-approach defining how to use various assessment methods to determine that a cloud service fulfils the requirements assigned to a given assurance level • two assessment methods defining how to determine that a cloud service fulfils a given set of requirements, as fully described in the scheme. • a set of document templates to be used during the evaluation and review activities to ensure that the documents released by the Conformance Assessment Body and its subcontractors follow the same organization and flow • a detailed list of the documents to be made publicly available as part of the certificate package, that may allow scheme users to locate the information they are looking for to make informed decisions • a set of rules about the lifecycle of certificates after their issuance, including maintenance and renewal requirements, management of vulnerabilities and complaints, and market surveillance activities, that may allow scheme users to remain informed of the evolution of the security of a given cloud service.

Focus Area	European Cybersecurity certification scheme for cloud services
Main characteristics of the EUCS	• It is a voluntary scheme • The certificate will be applicable across the EU Member States • It is applicable for all kinds of cloud services IaaS, PaaS, SaaS, and other cloud services • Boosts trust in cloud services by defining a reference set of security requirements • Covers three assurance levels: 'Basic', 'Substantial' and 'High' • Proposes a new approach inspired by existing national schemes and international standards • Defines a transition path from national schemes in the EU • Grants a three-year certification that can be renewed • Includes transparency requirements such as the location of data processing and storage
Benefits of the EUCS scheme for stakeholders	• a scheme harmonized at the European level • strong quality guarantees through the use of third-party assessment by accredited bodies, supervision by national authorities, and for the High level, authorization by the national authorities and peer assessment between conformity assessment bodies • the flexibility offered by three different assurance levels covering the entire range of assurance introduced in the EUCSA, with the possibility for a certified cloud service to upgrade to a higher level in future evaluation cycles • strong transparency guarantees, with security information made publicly available through a centralized web site • assurance maintained over time, with regular reassessments, operating effectiveness guarantees at the levels Substantial and High • a maintenance framework for the EUCS scheme, endorsed by European institutions and Member states, providing strong guarantees on continued operation of the scheme • integration in the European cybersecurity certification framework, which will facilitate the reuse of EUCS certified cloud services in vertical schemes.
Timeline	• The European Certification Scheme for Cloud Services was drafted and delivered in 2020 with the support of an Ad-Hoc Working group and the support of Member States. The text should now enter the process of the European Cybersecurity Certification Group for opinion.

[13] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).



The key legislative instrument on cybersecurity regulation is Law 4577/2018, which transposes the NIS Directive 2016/1148/EU into Greek legislation[14]. The Law sets out significant cybersecurity obligations for operators of essential services and providers of digital services. Businesses falling within the scope of the Law are required to (i) designate an information security officer; (ii) adopt technical and organizational measures for the security of networks and information systems; (iii) adopt measures to prevent and minimize the impact of incidents affecting the security of networks and information systems; and (iv) notify the National Cybersecurity Authority and the CSIRT of incidents with a serious impact on business continuity.

The statutory provisions of Law 4577/2018 are further specified and implemented by Ministerial Decision 1027/2019[15], which lays down in detail the information security requirements for obligated entities under the Law, provides for the information security incident notification procedure before the National Cybersecurity Authority, sets out the methodology of determining operators of essential services and stipulates the procedure and criteria for the imposition of sanctions. According to the Decision, obligated entities are required to execute self – assessments of the level of their information security by way of the National Cybersecurity Authority Self-Assessment Guide and Tool[16].

Furthermore, articles 15-27 of Law 4961/2022 set out the organisational framework for the designation of information security officers and the cybersecurity measures in the public sector. In addition, articles 20-33 of Law 5002/2022 lay down the rules for the adoption of a National Plan for the Evaluation of the Risk of ICT Systems and the establishment of a National Security Operations Center ("SOC").

Obligated entities are required under the Law 4577/2018 to establish and implement a cybersecurity organizational framework and technical infrastructure, so as to be able to achieve and sustain a high level of security in relation to their networks and information systems.

Finally, the Greek legislative framework on cybersecurity is supplemented by the provisions of Law 4411/2016[17], which transposed Directive 2013/40/EU on attacks against information systems and defines respective criminal offences and relevant sanctions.

[14] Government Gazette 199/A/ 03-12-2018, [15]Government Gazette 3739/B/08-10-2019, [16] Available: https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-English-version.zip., [17] Government Gazette 142/A/03-08-2016.

Focus Area	Greek Cybersecurity Law 4577/2018
Scope	• Operators of essential services in the fields of energy, transport, credit institutions, financial market infrastructure, health, water supply and digital infrastructures. • Providers of digital services, in particular e-commerce businesses and in general, digital services, search engines and cloud computing providers.
Key Requirements	Obligated entities are required to: • Adopt a general information security policy and designate an information security officer. • Implement technical and organizational requirements in respect of risk identification, information security protection and incident management and mitigation. • Notify incidents with a serious impact on business continuity without undue delay before the National Cybersecurity Authority and the CSIRT and towards the recipients of affected services.
Enforcement	The National Cybersecurity Authority has the following powers and competencies: • To assess the compliance of obligated entities with Law 4577/2018. • To order obligated entities to provide the necessary information, including security policies. • To order obligated entities to correct any breach of compliance. Following an opinion by the National Cybersecurity Authority, the Minister of Digital Governance may impose fines: • of up to EUR 15,000 in the event of no notification / delay of notification; • of up to EUR 50,000 in case of non-provision or unjustified delay in the provision of information or in the event of failure to take required measures; • of up to EUR 200,000 in case of recidivism.
Timeline	• Issuance of Ministerial Decision on security requirements and notification procedure before the National Cybersecurity Authority • Publication of National List of Obligated Entities under the Law 4577/2018 • Adoption of National Plan for the Evaluation of the Risk of ICT Systems

Within the two-year period up to the entry of DORA into application, **financial entities and market players in the FinTech ecosystem** will be required to upgrade their information security frameworks in order to be in line with the stricter requirements of the Regulation.

Apart from horizontal requirements applicable to essential service operators and digital service providers, EU and Greek cybersecurity law establishes sectoral obligations for the financial and electronic communications sectors.

In specific, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("DORA") lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities. The DORA constitutes the most ambitious initiative of the EU up to date to ensure security and resilience of the European financial sector in conditions of rapid digital transformation. In addition, the DORA grants new wide-ranging powers to national and European supervisory authorities for the oversight of critical ICT third-party service providers. A key aspect of the DORA is also its delegation to the ESAs to enact the secondary rules which will render possible the operationalization of the security framework of the Act. In order to promote innovation, the Regulation also allows for a proportionate set of obligations for financial entities which are qualified as micro enterprises and the application of the principle of proportionality in the supervision of its implementation by market players.

Focus Area	DORA
Scope	Credit and financial institutions, crypto-asset service providers, trading venues and repositories, investment firms, managers of alternative investment funds, management companies, credit rating agencies, data reporting service providers, crowdfunding service providers and, also, ICT third-party service providers
Key Requirements	• ICT incident reporting • Digital operational resilience testing • Information and intelligence sharing in relation to cyber threats and vulnerabilities • ICT third party risk management
Enforcement	Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.
Timeline	• The DORA has entered into force on 27 December 2022 • The Regulation shall apply from 17 January 2025 • The Commission will adopt Delegated Acts for the establishment of the critical supplier supervision framework of the Regulation • Within 24 months from its entry into force, ESAs shall jointly issue the Regulatory Technical Standards ("RTS") and Implementing Technical Standards ("ITS") of the Regulation

On the other hand, articles 109-223 of Law 4727/2020, which transpose Directive (EU) 2018/1972 on the European Electronic Communications Code[18] into Greek legislation, set out the cybersecurity requirements in the electronic communications sector. According to the relevant provisions of Law 4727/2020, electronic communication network and / or service providers are required to take information security measures, as these are determined by the decisions of the Hellenic Authority for Communication Security and Privacy[19]. They are also obliged to notify information security incidents to the Authority and, when these have serious impact, also to affected users of their networks. In addition, article 24 of Law 4961/2022 provides that electronic communication network providers are obliged to have in place cyber-risk assessment and procurement plans regarding their radio communication equipment.

Furthermore, with the aim to ensure the roll-out of secure 5G mobile communication networks and services across the continent, the European Commission has established in January 2020 the EU 5G Toolbox with the support of ENISA[20].

Focus Area	Law 4727/2020
Scope	Electronic communication network and / or service providers
Key Requirements	Obligated entities are required to: • take appropriate technical and organisational measures to manage security risks and prevent security incidents influencing their networks and services • notify information security incidents to the Hellenic Authority for Communication Security and Privacy and, in case of serious impact, to affected users • implement cyber-risk assessment and procurement plans in respect of radio communication equipment
Enforcement	The Authority for Communication Security and Privacy has the following powers: • to issue regulations regarding the assurance of the confidentiality of communications • to perform audits on communications network/service providers • to impose fines up to EUR 1.500.000
Timeline	• Law 4727/2020 has entered into force on 23 September 2020 • Greece is required to take further initiatives in order to ensure the secure deployment of 5G networks in the country according to the requirements of the EU 5G Toolbox

The Toolbox identifies a common set of measures to mitigate **the main cybersecurity risks of 5G networks** to be implemented in mitigation plans at national and at Union level.

[18] *OJ L 333, 27.12.2022, p. 1–79, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.*
[19] *See e.g. HACSP Decisions no. 165/2011 for the Assurance of confidentiality in Electronic Communications (GG 2715/B/2011) and no. 205/2013, Electronic Communications Network Security and Integrity Regulation (GG 1742/B/2013).*
[20] *NIS Cooperation Group, Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures, Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468.*

Finally, articles 32-42 of Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions"[21] establish a robust framework of rules for the information security of Internet of Things ("IoT") devices. The provisions of the law enact an advanced set of information security obligations for manufacturers, importers, distributors and operators of IoT devices, among others the incorporation of appropriate security measures in devices and the appointment of IoT security officers. The National Cybersecurity Authority is designated as the competent authority to oversee the IoT security framework implementation of Law 4961/2022.

Focus Area	Law 4961/2022
Scope	Manufacturers, importers, distributors and operators of IoT devices.
Key Requirements	• IoT manufacturers are required to incorporate measures that ensure an appropriate level of cybersecurity in their devices[22] • IoT manufacturers, importers and distributors are obliged to accompany IoT devices with a declaration of compliance with the technical safety specifications, indicated in the law • Each manufacturer should have a IoT device management process for cases where it is ascertained by the user that: a) a security incident occurs, or b) a vulnerability exists in the security parameters of the device. • IoT operators are required to (i) follow the technical safety specifications of each device; (ii) appoint an IoT Security Officer to monitor respective security measures; (iii) maintain a register of interconnected IoT devices; (iv) carry out data protection impact assessments; and (v) provide guidance and information to users on information security matters.
Enforcement	The National Cybersecurity Authority has the following powers: • To require from manufacturers, importers or distributors of IoT devices to take all necessary corrective actions in order to comply with the applicable legislation. • To order the temporary withdrawal from the market of IoT devices presenting risks and their re-placement in the market only if such risks have been removed. • The Ministry of Digital Governance may impose penalties of up to € 15,000 and, in case of recidivism, of up to € 100,000 in case of violation of the law.
Timeline	• Law 4961/2022 has entered into force on 27 July 2022 • The Minister of Digital Governance shall adopt decisions on the technical specifications and safety measures of IoT technology devices, the obligations of manufacturers, importers and suppliers of such products as well as the relevant sanctions in case of non-compliance.

> For the supply of IoT devices and / or the provision IoT – related services in the Greek market, businesses active in the national IoT ecosystem are required to establish **appropriate information security frameworks** in line with the provisions of the law.

[21] *GG 146/A/27-07-2022.*

[22] *Specific cybersecurity measures for IoT devices will be stipulated in a forthcoming Decision of the Minister of Digital Governance.*

3.4 Regulatory Developments

In line with the Commission Cybersecurity and Digital Compass strategies, EU institutions have adopted or are bound to adopt significant legislation in the field of cybersecurity, the most important of which are the NIS2 and CER Directives and the Cyber-Resilience Act.

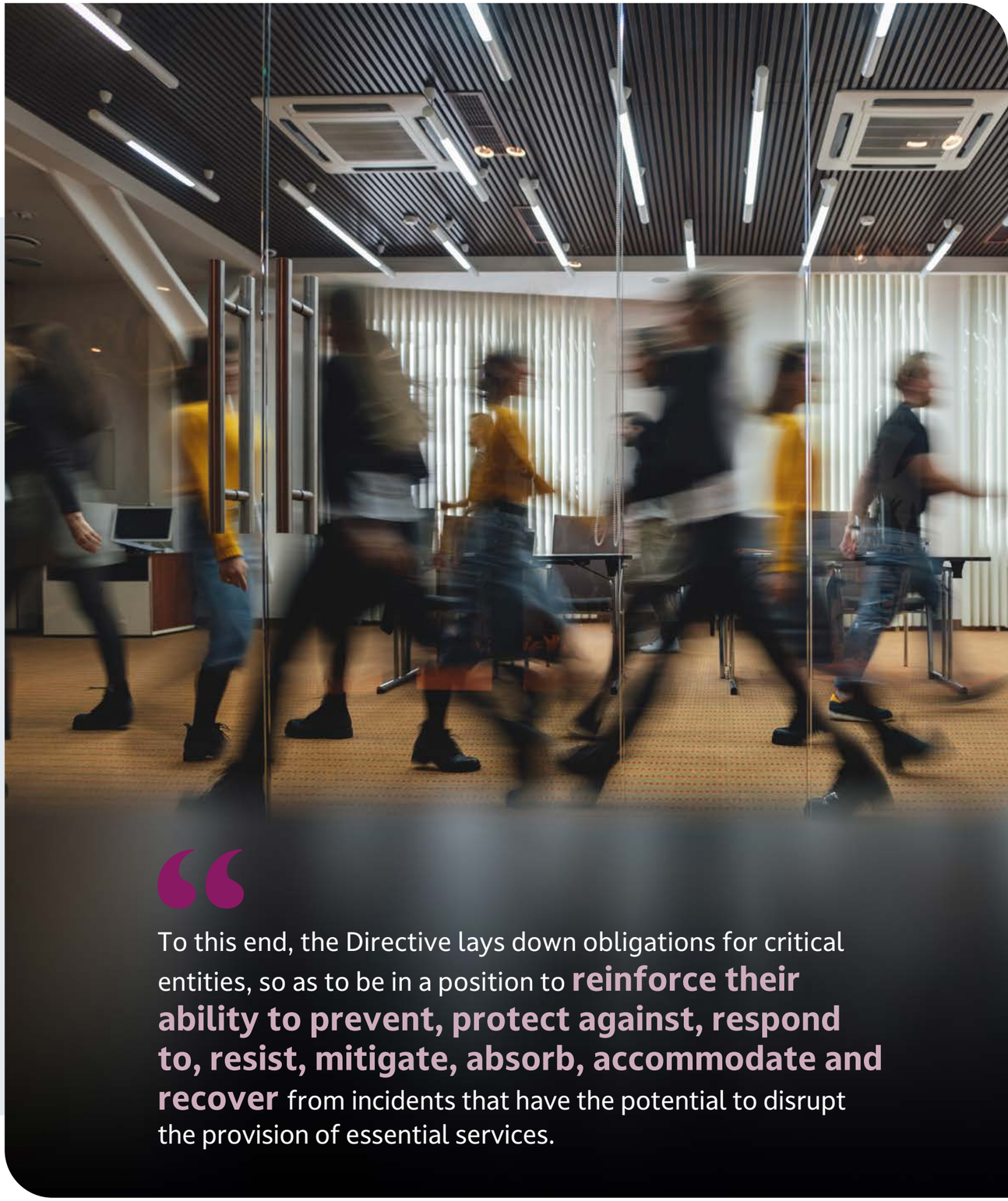
The NIS2 Directive[23] replaces Directive (EU) 2016/1148 ("NIS Directive") with the explicit purpose of achieving a high common level of cybersecurity across the Union and, in this manner, of improving the overall functioning of the internal market. In comparison to the NIS Directive, NIS2 expands the material scope of cybersecurity obligations to new categories of entities, establishes common advanced cybersecurity schemes and institutions of coordination and cooperation between member states, upgrades cybersecurity risk management and incident reporting requirements and, finally, provides for adequately deterrent powers of enforcement to Supervisory Authorities. By becoming applicable to medium and large enterprises, the NIS2 Directive extends the scope of cybersecurity obligations to a large part of the economy and is therefore expected to significantly improve the resilience of the public and private sectors.

[23] *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"), available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.*

Focus Area	NIS II Directive
Scope	• Medium and large enterprises (with more than 50 employees and an annual turnover greater than 10 million euros) • Critical entities falling within the scope of the CERD • Electronic communications network or service providers • Trust service providers • Top-level domain name registries and domain name system service providers • Entities which are the sole provider of a service in a member state or the services of which could have an impact on public safety, security or health if disrupted or could induce systemic risks or have cross-border impacts if disrupted • Public administration entities
Key Requirements	• Policies on risk analysis and information system security. • Business continuity, disaster recovery and crisis management. • Supply-chain security, including security-related aspects concerning the relationships between each entity and its suppliers or service providers • Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure • Policies and procedures to assess the effectiveness of cybersecurity risk-management measures • Cyber hygiene practices and cybersecurity training. • Policies on the use of cryptography and encryption • Cybersecurity risk assessment human resources security, access control policies and asset management • The use of multifactor authentication or other authentication solutions • Incident reporting obligations, according to which covered entities are required to notify CSIRTs or competent authorities and recipients of their services about incidents that significantly impact their ability to provide services, including an early warning, within 24 hours of becoming aware of the significant incident and an incident notification, within 72 hours there from.
Enforcement	Competent authorities have the following powers under the Directive: • Conduct off-site and on-site inspections • Impose administrative fines of up to 10 million euros or 2% of the company's total annual worldwide turnover, whichever is higher • Order the publication aspects of non-compliance and / or to suspend certifications and authorizations for services provided by the entity • Impose temporary ban of any individual responsible for the breach from management positions within the entity
Timeline	• The NIS 2 Directive has entered into force on 16 January 2023 • Member states will be required to transpose the provisions of the Directive into their national law by 17 October 2024 • Member states shall establish a list of entities falling within the scope of the Directive by 17 April 2025 • The Commission shall publish guidelines for the application of Article 4 (1) and 4 (2) of the Directive by July 17,2023

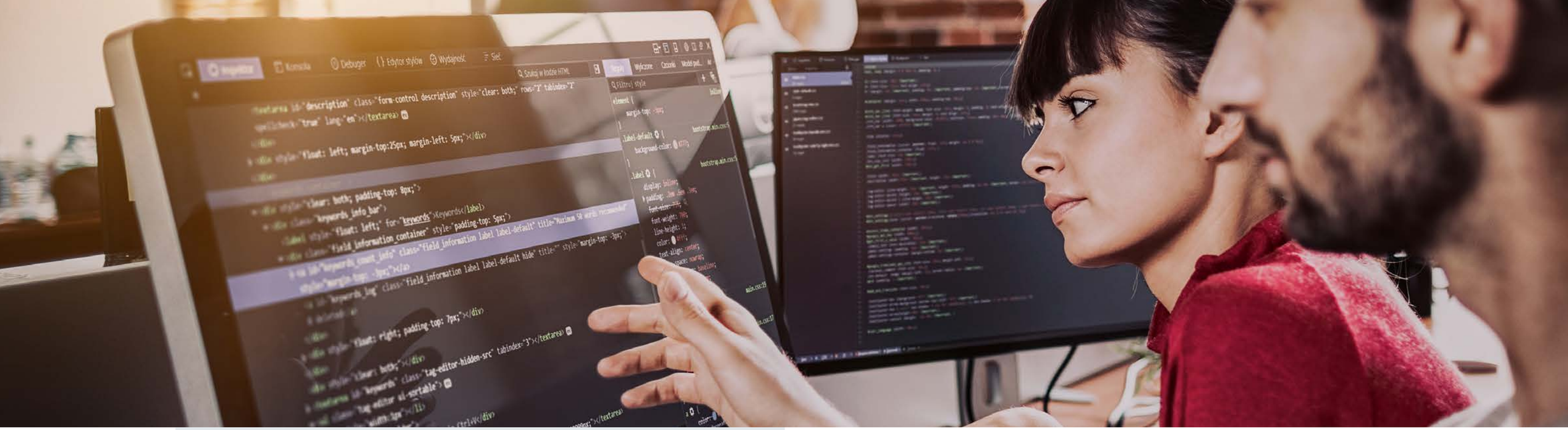
The Critical Entities Resilience Directive ("CERD")[24] sets out a harmonized framework of rules for the enhancement of the resilience of critical entities in the European internal market. The CERD aims to address the dynamic threat landscape for critical infrastructures at national, European and global level, which includes evolving hybrid and terrorist threats, increased physical risk due to natural disasters and climate change and growing interdependencies between infrastructure and sectors.

Focus Area	CERD
Scope	Operators of essential services in the sectors of energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space and production, processing and distribution of food
Key Requirements	Critical entities are obliged to take the following measures to ensure the resilience of their essential services (Chapter III CERD): • execute risk assessments regarding the risks that could disrupt the provision of their essential services • take appropriate and proportionate technical, security and organisational measures to ensure their resilience • conduct background checks on natural persons capable of influencing the level of their resilience • notify competent authorities, without undue delay, of incidents that may significantly disrupt the provision of essential services
Enforcement	Competent national authorities shall have the powers and means to: • require information and evidence about measures taken by critical entities • conduct on-site inspections of the critical entities' infrastructure and premises • supervise measures taken by critical entities • conduct or order audits in respect of critical entities • impose effective, proportionate and dissuasive penalties applicable to infringements and take all measures necessary to ensure that measures are implemented
Timeline	• The CERD has entered in force on 16 January 2023 • Member states are required to transpose the Directive into national law and adopt national CER strategies by 17 January 2026 • Member states are required to establish national lists of critical entities by 17 July 2026



"To this end, the Directive lays down obligations for critical entities, so as to be in a position to **reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover** from incidents that have the potential to disrupt the provision of essential services.

[24] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, p. 164–198, available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj*



> From its entry into force, manufacturers and businesses across the supply chain of products with digital elements will be given a two-year period **to establish the technical and organizational security measures** that are required by the Act.

The Cyber Resilience Act is a proposal for a Regulation by the European Commission which imposes horizontal cybersecurity requirements for hardware and software products with digital elements with the aim to bolster the security of such products within the internal market. According to the Act, when placing a product with digital elements on the market, manufacturers are required to ensure that it has been designed, developed and produced taking into account essential cybersecurity requirements and perform a conformity assessment of the product. On the other hand, importers may only place on the market products with digital elements that comply with the essential requirements of the Act and distributors must act with due care in relation to the requirements of this Regulation. In addition, each product with digital elements ought to be accompanied by a certain set of information and instructions to the user related to cybersecurity. Furthermore, critical products with digital elements will need to comply with advanced cybersecurity requirements. Finally, manufacturers should report vulnerabilities and information security incidents of their products to ENISA within 24 hours of becoming aware.

Focus Area	Cyber Resilience Act
Scope	Manufacturers, authorised representatives, importers, distributors of product with digital elements
Key Requirements	• General product safety requirements and essential cybersecurity requirements • Cybersecurity by design and throughout the manufacturing phases of products • Execution of cybersecurity risk assessment reports and conformity assessments • Effective handling of vulnerabilities for the expected product lifetime or for a period of five years from the placing on the market • Reporting of vulnerabilities and information security incidents to ENISA within 24 hours of becoming aware • Clear and understandable instructions for the use of products with digital elements • Security updates to be made available for at least five years
Enforcement	• Non-compliance with essential cybersecurity requirements shall be subject to administrative fines of up to 15 000 000 EUR or 2.5 % of the total worldwide annual turnover for the preceding financial year, whichever is higher • Non-compliance with any other obligations shall be subject to administrative fines of up to 10 000 000 EUR or 2 % of the total worldwide annual turnover for the preceding financial year, whichever is higher
Timeline	Economic operators will have two years from entry into force to adapt to the requirements of the Act

[24] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, p. 164–198, available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj*

4 Current cybersecurity challenges in the Greek market

The overall legal and regulatory landscape aims to increase **the cyber resilience of organizations** across all sectors and industries and reduce the overall cybersecurity risk

4.1 Overview of cybersecurity challenges

Over the last few years, Greece have made significant efforts towards enhancing its digitalization capabilities through a number of appropriate initiatives. It is evident however, that the cybersecurity legal and regulatory landscape is quite extensive, bringing forward several requirements and responsibilities, which are often overlapping, thus posing various compliance challenges for the Greek companies.

These compliance challenges can be derived from the following four main sources:

- Fragmentation of the regulatory and legislative landscape
- Organizational and administrative concerns
- Management of third-party compliance
- Availability of talent/skills to effectively manage cybersecurity compliance

More specifically, the overall legal and regulatory landscape aims to increase the cyber resilience of organizations across all sectors and industries and reduce the overall cybersecurity risk. However, the relevant official legal and regulatory systems which are in place and are tasked with creating the appropriate regulations and legislative frameworks are striving to adapt to the speed at which new technologies are introduced, and thus create an overall landscape which is fragmented and ultimately quite challenging to effectively manage.

The administrative effort, including time and costs as well as overall skills, talent development and training required by organizations to ensure that they are compliant with the expanding requirements, also proves challenging to manage. The issue is exacerbated when the aspects of rapid digitalization and relevant technological advancements, especially in a post-COVID-19 environment, combined with concerns involving the degree of management involvement and commitment to cybersecurity, as well as the available budget and relevant investments, are taken into account.

Finally, and due to the aforementioned speed at which technological advancements are introduced, organizations are more likely to become increasingly dependent on third parties to more efficiently adopt them and thus adapt to the ever-changing landscape. Such dependencies on third parties, however, potentially increase the associated compliance risks, as a result of the varying degrees of their maturity levels and the lack of establishment of proper third-party monitoring and management mechanisms.

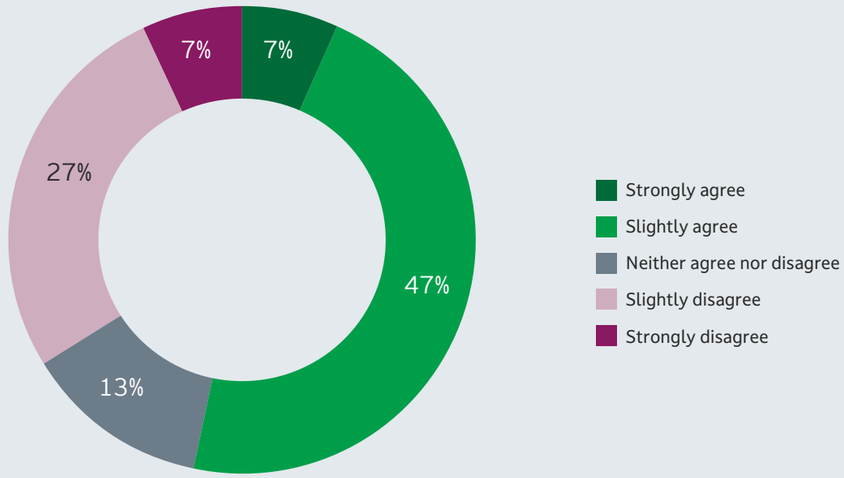
4.2 Cybersecurity challenges in the Greek market

In the context of the current report, a Questionnaire had been disseminated to cybersecurity professionals in multiple organizations across different sectors and industries, in order to more accurately identify the challenges they face, as a result of the relevant cybersecurity legislation and regulations.

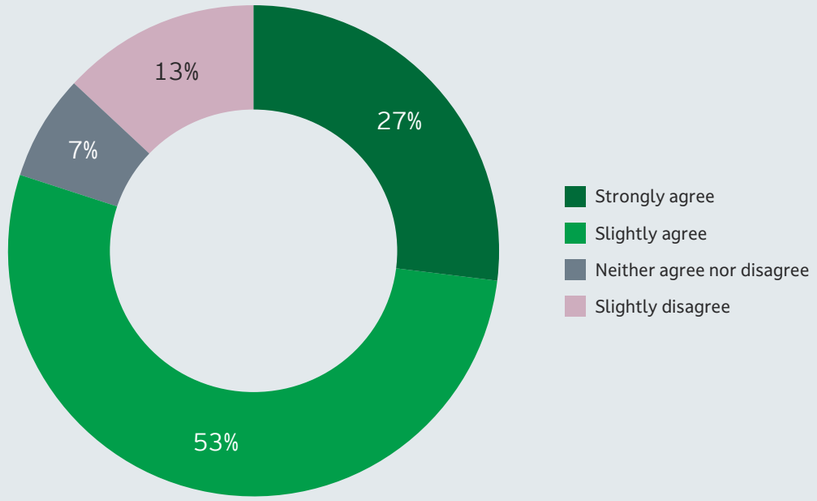
Based on the responses received, it has been noted that all of the respondents assess that cybersecurity regulations generally contribute to reducing their organization's risk, generally constituting positive drivers in effective decision-making and relevant investments, while the vast majority of respondents also agree that compliance requirements effectively promote an appropriate cybersecurity culture within the organization. Additionally, slightly more than half of the participants also considered that the administrative costs required to ensure compliance with the cybersecurity regulatory landscape are a burden to their respective organizations.

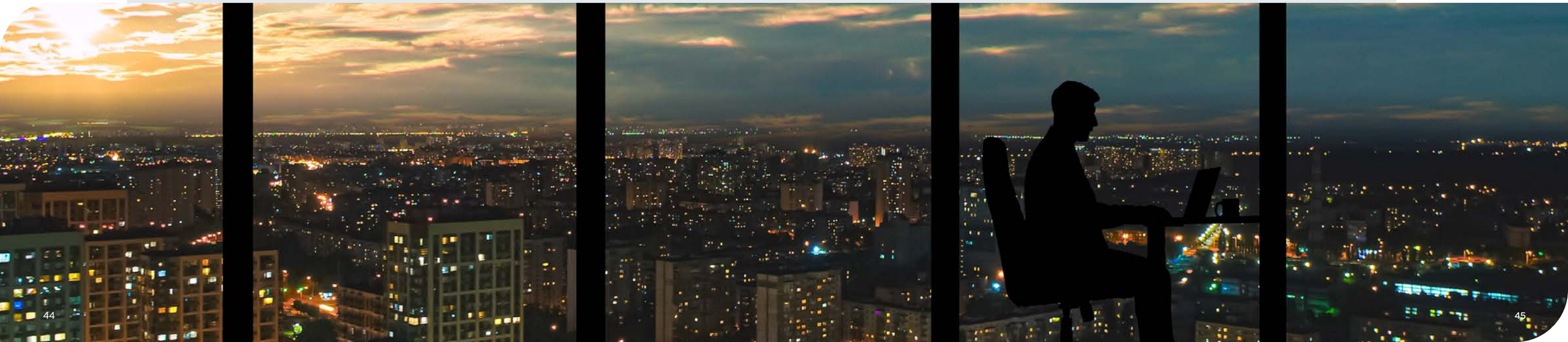
Despite that, however, the majority of the respondents do agree that the regulatory landscape is fragmented, with conflicting and overlapping requirements, therefore being time-consuming and complicated to manage, while also stating that the effort, resources, skills, tools, and the relevant costs required to ensure their organization's compliance with the cybersecurity regulatory requirements are not properly estimated in a timely manner. In addition, most of the respondents agree that, ultimately, keeping up with changes in the cybersecurity regulatory landscape is difficult and time consuming, although there is a high degree of uncertainty on whether demonstrating compliance to it would be considered to be the most stressful part of their job.

The administrative time and costs required to ensure compliance with the cybersecurity regulatory landscape are a burden to the organization



The Cybersecurity Regulatory Landscape is Fragmented

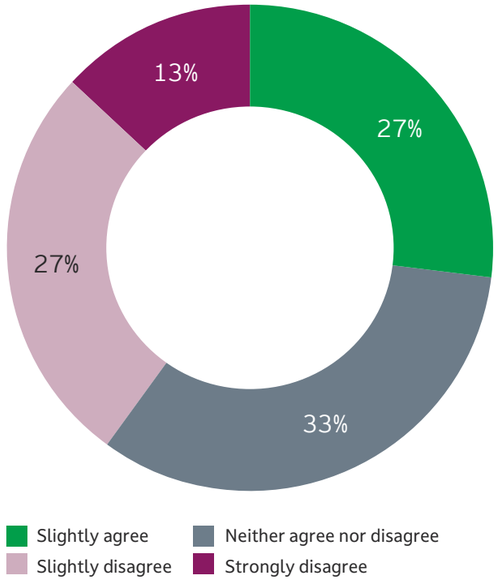




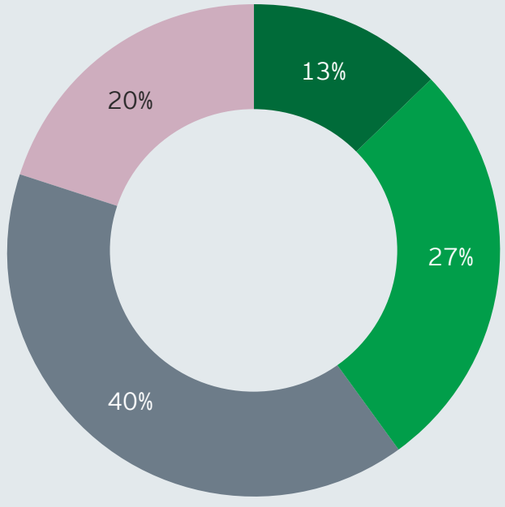
About half of the respondents have also stated that they are confident in their respective organizations' ability to manage the compliance requirements they are mandated to address as a business, while almost all of them agree that the overall regulatory landscape has made their job easier, especially in justifying the need for new cybersecurity initiatives. At the same time, however, the majority of the respondents stated that additional cybersecurity investments are required to enhance their position against the regulatory authority in the event of an audit, regarding their organization's compliance with the applicable cybersecurity requirements.

Separately, in terms of third-party management, the majority of respondents agree that increased dependency on third parties may pose a significant compliance risk, as their overall maturity may vary, while there is a high degree of uncertainty on whether their respective organization has a clear view and control over the relevant third parties in order to properly manage the associated compliance risks.

The organization has a clear view and control over third parties in order to properly manage the associated compliance risks



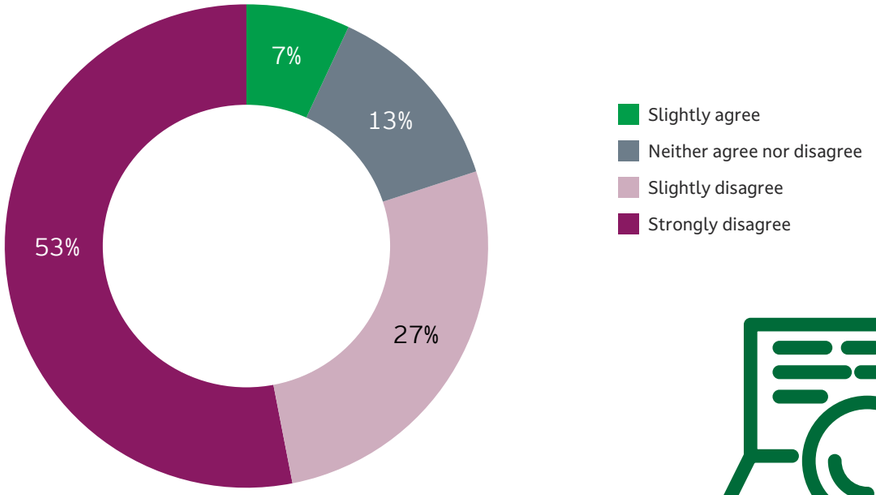
The organization has a clear view and control over third parties in order to properly manage the associated compliance risks

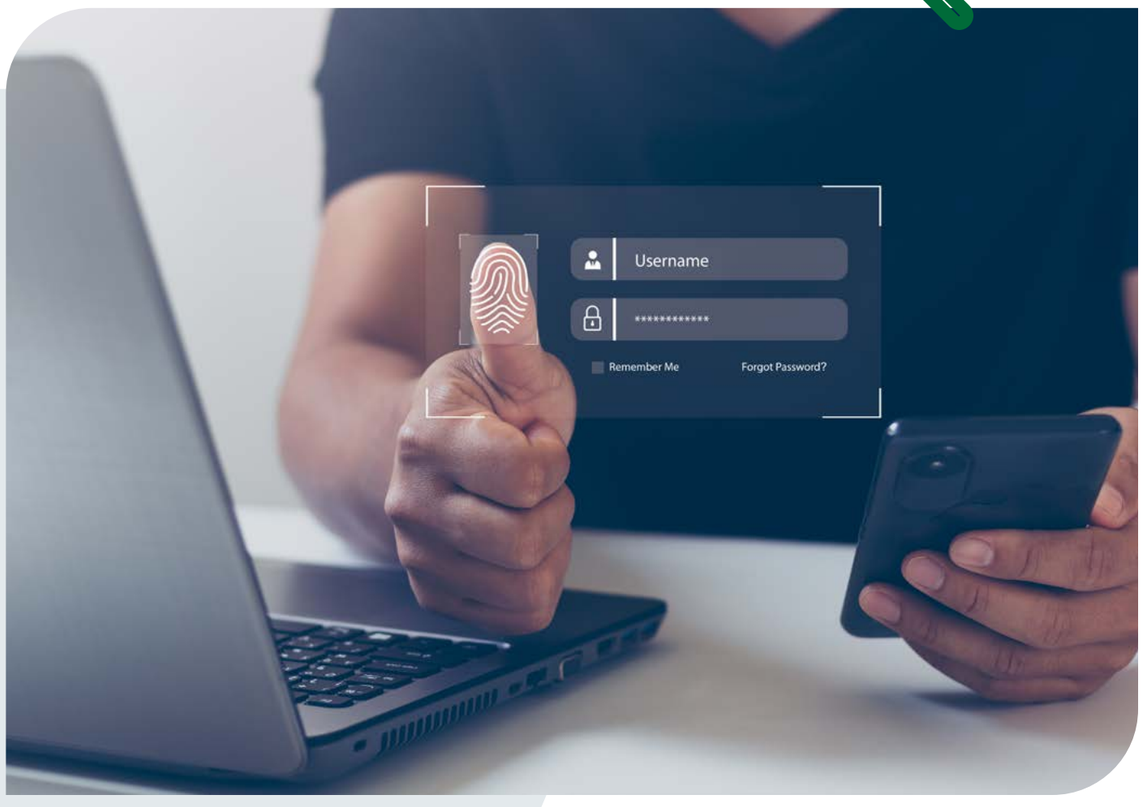


Regarding the effects of COVID-19, the majority of respondents have stated that the risk of non-compliance with the regulatory landscape has increased as a result of the pandemic and the establishment of the hybrid working environment while, at the same time, they largely support that the business rolls out new technology to urgent timescales that do not allow time for suitable assessment or oversight from the perspective of regulatory compliance. Additionally, there is a high degree of uncertainty on whether the business has implemented appropriate technology controls and relevant tools to achieve and continuously monitor its compliance.

Finally, most of the participants have assessed that finding the appropriate resources in terms of talent or skill to effectively address compliance concerns is challenging.

It is relatively easy to find appropriate resources to effectively address compliance challenges





The latest EY's Global Information Security Survey (GISS) largely corroborates the above findings:

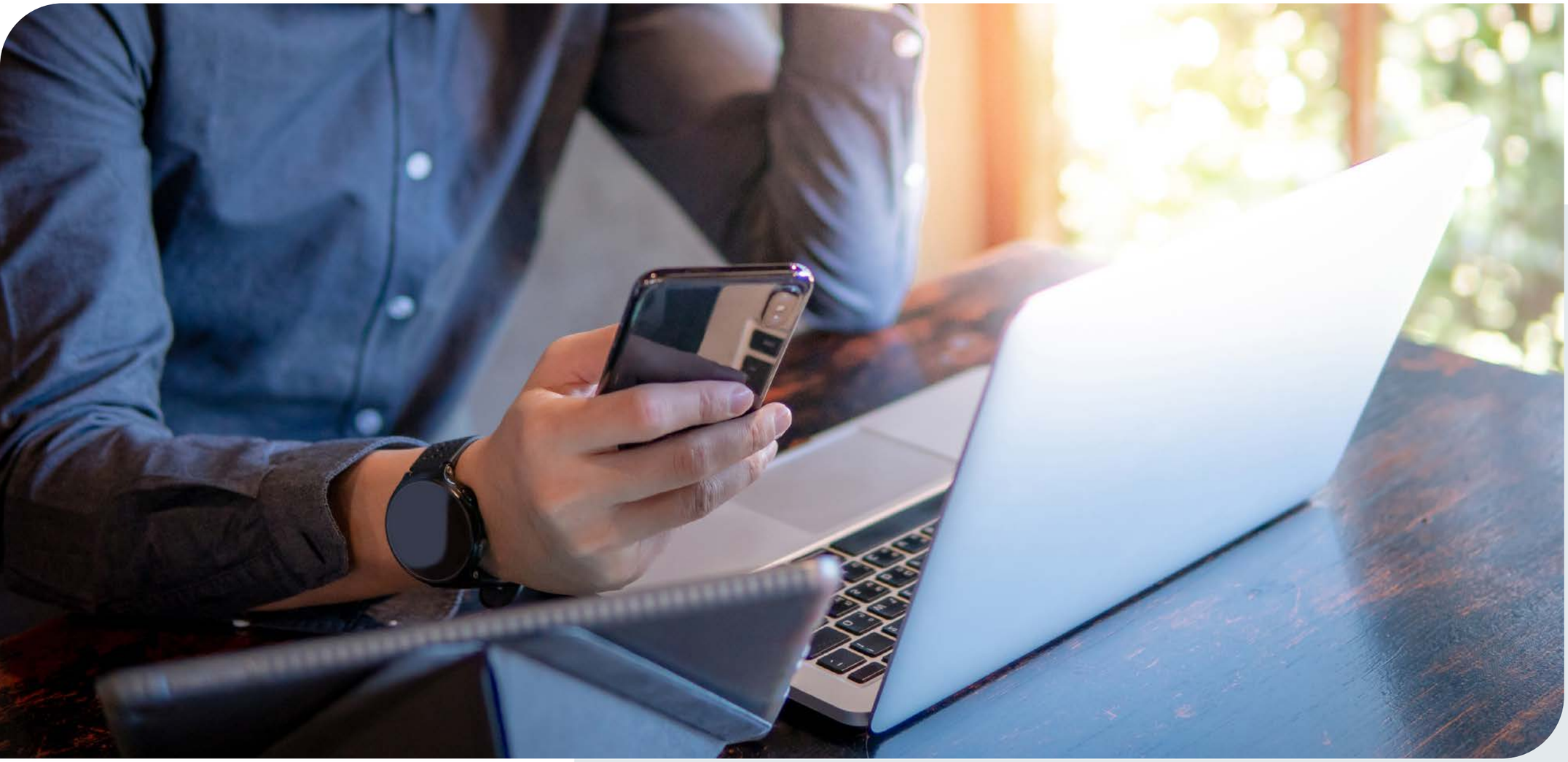
- The vast majority (87%) of respondents worldwide agree that, generally speaking, cybersecurity compliance requirements, either industry-specific or government-driven, drive the right focus and behaviors within their organization.
- Despite this, however, about half of respondents (51%) have assessed that ensuring and managing compliance in the context of the increasingly fragmented regulatory landscape is one of the most complicated aspects of the job,
- Most of them (60%) anticipate that the aforementioned regulatory landscape will become even more fragmented and therefore more time-consuming to manage in the future.

Based on these challenges, and according to the same responses, the actions taken to address them include:

- Improvement of governance capabilities and prioritization through the implementation of new technologies
- Increased appropriate resources
- Frequent process reviews, field testing and relevant follow up exercises
- Conducting training and awareness campaigns
- Establishment of stronger risk and compliance management methodologies
- Performance of gap analysis where necessary
- Stronger emphasis on automation
- Adoption of industry best practices through the relevant frameworks
- Collaboration with experts in the field of cybersecurity

Summarizing the provided responses, it is clear that while cybersecurity regulations constitute positive contributors in reducing the organizations' overall cybersecurity risk through more effective decision-making and the establishment of a stronger cybersecurity culture, the landscape is estimated to become even more fragmented and thus more challenging to effectively manage.

While most organizations have been taking the necessary steps to address this challenge, the issue is further exacerbated by the fact that most organizations assess that there is a lack of skilled professionals and management commitment, combined with budgetary concerns and an overall difficulty in identifying the relevant regulatory requirements as a result of the increasing degree of fragmentation.



5 How Microsoft can help you address these challenges

Microsoft Defender for Cloud aims to improve the organizations' overall cybersecurity posture.

5.1 Products

Microsoft's suite of cloud and security-oriented products is built to assist organizations across all industries and sectors in their digital transformation journeys while addressing the relevant challenges that may arise. Companies can leverage Microsoft's integrated security features both in the cloud and on-premises to improve their security capabilities across the board.

More specifically, Microsoft Defender for Cloud aims to improve the organizations' overall cybersecurity posture by providing a centralized security posture management solution to effectively monitor workloads and receive tailored security recommendations based on correlation processes made possible through the integrated security analytics engine. The solution supports the following capabilities:

- Centralized policy management, assisting in the identification of violations to the established security policy based on set security conditions
- Multicloud coverage by allowing connection to the relevant environments with agentless methods
- Cloud and Advanced Cloud Security Posture Management (CSPM) through the dashboard
- Data-aware Security Posture, allowing the automatic discovery of datastores containing sensitive data
- Security governance and improvement, by assigning tasks to resource owners and tracking alignment progress between the security state and the established security policy

The establishment of remote work as a result of the pandemic, as well as the rise of nation-state attacks and the increasingly evolving regulations, have dictated the need to allow the creation of a holistic, up-to-date mapping of the data landscape with automated data discovery, sensitive data classification and end-to-end data lineage and thus enabling organizations to define a unified map of data assets along with their relationships for more effective data governance. More specifically, Microsoft Purview supports the following capabilities:

- Enhanced detection and investigation capabilities through Insider Risk Management
- Document and data discovery through eDiscovery, allowing organizations to respond to both internal investigations and external inquiries
- Code of conduct violations' detection capabilities through Communication Compliance
- Unified data governance and compliance capabilities, through Data Lifecycle Management, Data Loss Prevention and Information Protection solutions.

Separately, Azure Monitor provides a comprehensive solution to enhance cloud security capabilities and the organization's overall cloud adaptability and scalability by collecting, analyzing and responding to telemetry from cloud and even on-premises environments. The solution provides the following capabilities:

- Improved monitoring and observability, by collecting data from multiple data sources and data platforms
- Monitoring data routing through a set of different mechanisms depending on data and destination
- Curated visualization capabilities providing insights for web applications, containers, Virtual Machines (VMs) and network resources through dashboards, workbooks, Power BI and Grafana
- Analysis of monitoring data through the metrics explorer interface, log analytics and change analysis
- Response capabilities through automated processes, leveraging Alerts, Autoscale and Azure Logic Apps functions to receive notifications, dynamically control the number of resources running and to create automated workflows

Finally, security solutions such as the Microsoft 365 Defender suite and Microsoft Sentinel can be utilized to safeguard endpoints, applications and services both in the cloud and on-premises, leveraging the relevant SIEM and extended detection and response capabilities (XDR) to improve efficiency and effectiveness while allowing companies to properly secure their digital estate.

5.2 Cases

From banking to consumer goods, manufacturing and energy, organizations in various industries use Microsoft products and services to meet compliance obligations in a dynamic regulatory landscape. The success stories below showcase how some of the largest companies in Greece and other countries managed to address the challenges deriving from this complex landscape with Microsoft's help.

i) Tighter integration between security layers to boost protection

Who: MSC Mediterranean Shipping Company S.A. (MSC)

What: MSC needed efficient ways to keep its ships, cargo, and data safe wherever they are. Integrating security features in Microsoft 365 allowed the company to reinforce its security layers, identify hidden risks both on-premises and in the cloud, and automate routine tasks so its security team can focus on innovation.

How: The organization has deployed Microsoft 365 E5, including Windows 10 Enterprise, Office 365 and Enterprise Mobility + Security, leveraging the interoperation capabilities among the provided security products to strengthen and streamline its defenses. Azure Security Center is considered the company's "one-stop-shop" for the entirety of its Azure infrastructure, covering more than 750 virtual machines and being able to utilize it with the on-premises infrastructure as well. Azure Active Directory (Azure AD) is also deployed to manage identity and access management, utilizing its Privileged Identity Management and Identity Protection features, while Azure Information Protection and Microsoft Threat Protection are leveraged to respectively facilitate compliance with the relevant regulations as well as the timely detection of, and response to, threats.

ii) Leveraging Azure capabilities to lay the foundations for long-term growth

Who: Metinvest

What: The company needed to scale and expand the capacities of its existing data centers. Supported by Metinvest Digital, which is its IT and innovation partner, the group forged a strategic alliance with Microsoft and Infopulse to move 680 servers to Azure.

How: Metinvest leverages the Azure Security Center capabilities for advanced threat protection and unified security management, through monitoring and maintaining security in the cloud via the Azure Monitor and Security Center solutions, allowing all services to connect to it, and providing a holistic view of subscriptions, tenants and activities while, additionally, Azure Bastion is utilized to ensure secure access to servers while Azure Files has replaced the company's on-premises file servers, ensuring fully managed, shared access to company files.

iii) Use of Microsoft Security solutions to reimagine banking for a digital audience

Who: ING Bank

What: A long history and varying regulations around the world complicated the IT landscape for ING. Its proactive IT team knew that consolidation was key to improving security, but it needed a coordinated security solution to protect its digital assets

How: The bank rolled out Microsoft Security solutions such as Microsoft Sentinel for SIEM and extended detection and response (XDR) capabilities and the Microsoft Defender suite to protect endpoints, identities, and cloud apps. Microsoft Defender for Cloud provides a single pane of glass view into ING's multi-cloud environment, which is achieved by using Azure Arc to capture all the logs and signals from its platforms. Microsoft Sentinel then analyzes the logs and signals, enabling the company's security analysts to review and respond to potential threats quickly and proactively. With Microsoft Defender for Endpoint and Microsoft 365 Defender, including e-mail protection, ING expanded its XDR strategy. With its intense focus to meet every regulatory requirement, ING is now installing Microsoft Purview Compliance Manager and testing Microsoft Purview Data Loss Prevention.

iv) Zero Trust strategy supported by Microsoft Security solutions

Who: Siemens

What: When Siemens began to transition to the cloud, it emphasized real-time, proactive security in order to apply a Zero Trust approach. It needed a tightly coordinated set of security solutions to protect identities, data, and endpoints.

How: Already committed to the productivity-enhancing apps in Microsoft 365, Siemens starts its Zero Trust strategy by securing three areas: identities (including access by external parties), data, and endpoints, and makes full use of the rich security built into the solution, including Azure Active Directory, Microsoft Defender for Identity, Microsoft Endpoint Manager, Microsoft Defender for Endpoint, and more. With Microsoft Defender for Identity Siemens protects and monitors its on-premises identities as well as data and devices by applying Conditional Access policies. Privileged Identity Management is applied to manage access to resources across Microsoft 365 and devices managed via Microsoft Intune, Azure as well as non-Microsoft software as a service (SaaS) applications. Siemens also utilizes Microsoft Information Protection to classify and protect data, and Microsoft Defender for Cloud Apps to manage data sharing and access to resources and applications. The company will also roll out Microsoft Defender for Endpoint to locate configuration issues and vulnerabilities in real time, and to monitor and block threats to endpoints.

v) Overcoming a ransomware attack

Who: G&J Pepsi-Cola Bottlers

What: When G&J Pepsi-Cola Bottlers was hit by a Cobalt Strike ransomware attack, it didn't pay or lose data thanks to its adept restoration of its Microsoft Azure Backup files. After recovering from the attack, the company embarked on an extensive security upgrade.

How: The company doubled down on endpoint management with Microsoft Defender for Endpoint, Intune, and other Microsoft 365 Defender capabilities. After the ransomware was discovered, G&J Pepsi's security team used Microsoft Defender for Endpoint to identify and shut down all its compromised VMs, isolating every device suspected of being targeted for lateral movement by the hackers. Using Azure Backup, data in each server were restored, the company lost no data, it overcame security event monitoring limitations by hiring a managed detection and response responder and now uses Microsoft Graph Data Connect for easy visibility. As soon as the company recovered from the attack, an intensified cybersecurity program began, which refined an already sophisticated security posture and extending the use of Microsoft Defender for Endpoint and Microsoft Intune.

vi) Enhancement and streamline of data ownership and data sharing

Who: bp

What: The company's vast data platform has a vital role to play in bringing the vision for greater diversity & integration to its energy sources to reality, by enabling data sharing and data management across its BUs faster and more effectively than ever.

How: The bp Data Hub, a multi-cloud solution, is designed to integrate the entire data value chain and provide a consistent, persona-driven data experience across the company's Microsoft and third-party cloud environments. With Microsoft Purview, bp is working to provide unified multi-cloud data governance through automated data discovery, sensitive data classification, and end-to-end data lineage. Data sourced from anywhere within bp's data platform can consequently be verified, qualified, highly reliable, and secure by design. This will allow data sourced from users to ensure that their analytical and commercial uses for the data are as verified and qualified as possible. Larger volumes of data sourced from across the organization will soon be readily available with far fewer restrictions, allowing for the creation of an ecosystem of reusable companywide data products.

6 Moving forward

The digital landscape is rapidly changing. Unchecked technology advancements have opened the way for multiple new vulnerabilities which can be exploited by threat actors, who also leverage new technologies to introduce new and more sophisticated cyber threats. The increased adoption rate of new technologies, including in Operational Technology (OT) and Internet of Things (IoT), the Blockchain, as well as technologies leveraging Artificial Intelligence (AI) and Machine Learning (ML) capabilities, has created new threat and attack vectors across businesses, government organizations and individuals on a global scale.

In general, cyber-attacks have increased in number, severity, as well as in potential damage caused to the targets, aiming to disrupt not only businesses but nation-states' critical infrastructure as well. This poses a significant challenge to organizations as they need to ensure that they are able to keep up with, and ultimately balance between, adapting to new technologies and ensuring their cybersecurity at the same time.

The issue is further exacerbated when the overarching legislative and regulatory landscape is taken into consideration. The overall regulatory environment and the relevant compliance requirements derived from it, are becoming increasingly fragmented, as, similar to organizations, they also strive to keep up with the rapid technology advancements.

Microsoft aims to continuously deliver **innovative solutions**, priming its customers for the relevant technological advancements.

It is clear then, that organizations need to properly equip themselves to ensure that they are able to simultaneously adapt to new technology advancements, keep cybersecurity in check, and stay compliant with industry, government or regional regulatory requirements in an efficient manner. Thus, leveraging the right tools to facilitate the aforementioned aspects is key for day-to-day operations as well as in the long term.

Microsoft's suite of security solutions both for cloud, on-premises and hybrid architectures can be utilized by organizations across all industries and sectors to enhance their cybersecurity capabilities, facilitate regulatory compliance and allowing them to focus on business development. Simultaneously, Microsoft aims to continuously deliver innovative solutions, priming its customers for the relevant technological advancements. For instance, Microsoft's all-new Security Copilot, a security analysis tool leveraging Artificial Intelligence and Machine Learning capabilities, can enable organizations to respond to threats quickly, assess risk and process signals at machine speed, enhancing the overall incident response, threat hunting and security reporting capabilities across the board.

At the same time, Microsoft's expanded strategic alliance with EY assists companies in their pursuit of digital transformation by addressing the relevant business and regulatory challenges, allowing them to more effectively move to and innovate in the cloud, through the integration of EY's business and technology consulting offerings with Microsoft's security and cloud solutions.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com

ey.com

For more information please contact:

Panagiotis Papagiannakopoulos
Partner, Deputy CESA Cyber Security Services Leader,
EY Greece
T +30 210 2886 676
E panagiotis.papagiannakopoulos@gr.ey.com

Antonios Broumas
Senior Manager, Digital Law,
Platis - Anastasiadis & Associates Law Partnership, EY Law
T +30 210 6171 502
E antonios.broumas@gr.ey.com

Nikolaos Gargalis
Manager, Technology Consulting Cybersecurity,
EY Greece
T +30 210 2886 835
E nikolaos.gargalis@gr.ey.com

EY @EY_Greece EY Greece
eygreece EY Greece

Microsoft

Founded in 1975, Microsoft (Nasdaq “MSFT”@microsoft) enables the digital transition to the age of the intelligent cloud computing and the intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

Microsoft began its activities in Greece in 1992. During the last 30 years, Microsoft Hellas offers software, services, devices, and solutions that help people and organizations to reach their full potential. In 2020, Microsoft launched the Gr for Growth initiative, a major technological commitment to citizens, the Public sector and businesses of all sizes in Greece for technology and new resources that create additional growth opportunities.

Under this initiative, Microsoft will construct a complex of three Datacenters in Attica, placing the country on Microsoft’s global cloud infrastructure map – which is the largest in the world - thus ensuring access to business-level “low latency” Cloud services. At the same time, in order to support Greek citizens in their professional as well as personal goals, Microsoft will train a workforce of 100,000 citizens in digital skills by 2025.

microsoft.com

For more information please contact:

Dimitrios Patsos
CISSP, CISM, CDPSE, CCSK Sr Specialist,
Security Specialist Technology Unit
Microsoft Greece, Cyprus, Malta
T +30 211 1206 371
E dpatsos@microsoft.com

Dimitris Choustoulakis
Sr Partner Development Manager
Global Partner Solutions (GPS)
Southeast Europe, Microsoft
T +30 211 1206 152
E dichoust@microsoft.com

Stamatis Kasmas
Sr Business Strategy Manager
Data Centre Lead
Microsoft Greece, Cyprus, Malta
T +30 211 1206 038
E stamatis.kasmas@microsoft.com

Microsoft Microsoft
Microsoft Greece