EU Legislation on Cybersecurity
NIS 2, DORA, AI Act

- **Gabor Gabriel**
- Senior Architect

Different regulations – Different objectives

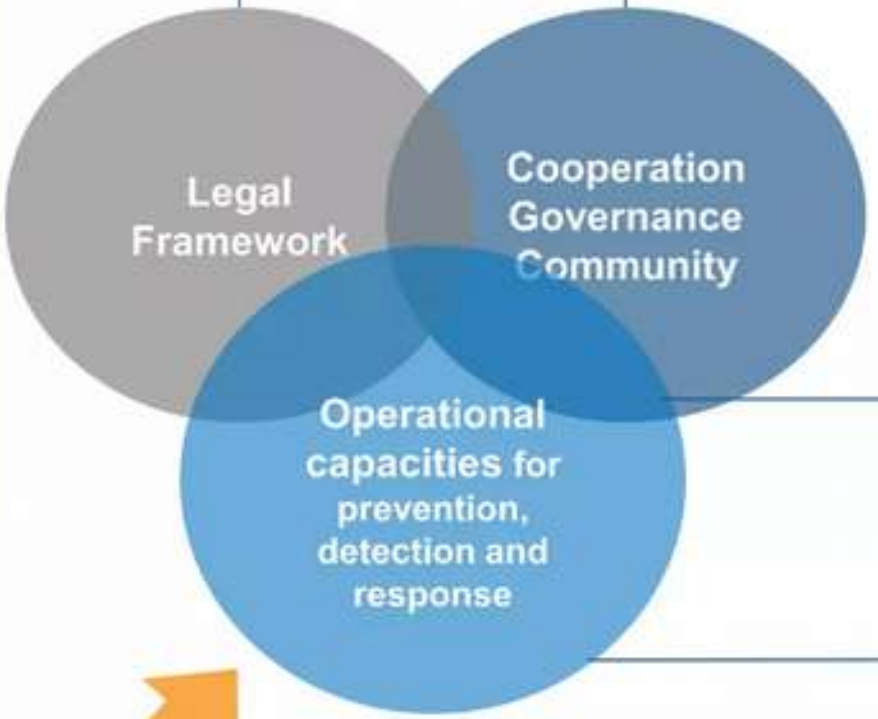
The goal of the NIS 2 directive is to ensure that **organizations vital to the proper functioning of our society achieve a high level of digital security**.

DORA aims to strengthen the **operational resilience of digital systems in the financial sector**. The implementation of the requirements in affected institutions aims at ensuring that financial institutions are able to withstand a cyber attack and continue to operate.

The AI Act is the first-ever comprehensive legal framework on AI worldwide. The aim of the new rules is to foster trustworthy AI in Europe and beyond, by **ensuring that AI systems respect fundamental rights, safety, and ethical principles** and by addressing risks of very powerful and impactful AI models.

EUROPEAN CYBERSECURITY CONTEXT

- Regulation 910/2014 eIDAS
- Regulation 2016/679 GDPR
- Regulation 2019/881 Cybersecurity Act
- Regulation 2021/887 ECCC
- Directive 2016/1148 NIS
- Directive 2022/2555 NIS2
- Directiva 2022/2557 resilience of critical entities (CER)
- Council Conclusions on security of the Supply Chain
- EU Policy on Cyber Defence
- Proposal Cyberresilience Act (CRA)
- Proposal Regulation DORA
- Proposal Regulation eIDAS2
- Proposal Regulation on Cybersecurity of EU Institutions
- Proposal Regulation on information security of EU Institutions
- Proposals European Certification Schemes (EUCC, EUCS)



- International Cooperation in Cybersecurity Standards & Specifications
- Cooperation with Third Countries
- Cooperation about Cybercrime and Cyberdefense
- NIS Cooperation Group
- European Cybersecurity Competence Center
  - Network of NCCs
  - Cybersecurity Community

- Joint Cyber Unit
- CSIRT Network (Directive NIS)
- CyCLONe – Crisis Management
- ...

- ENISA
- CERT-EU (for EU Institutions and Agencies)
- Quantum Computing, 5G,
- DNS4EU
- Cybersecurity exercises
- Rolling Program for ICT (Cybersecurity)...

+ Funding

- Digital Europe Programme - Cybersecurity
- Horizon Europe

(Non exhaustive)

Directive : not directly applicable in Member States, it must first be transposed into national law before it is applicable in each Member State

Regulation : directly applicable in Member States after its entry into force

NIS 2 Directive
Network & Information Security Directive

Introduction to NIS 2 Directive

Enhancing EU Cybersecurity

- **Purpose of NIS 2 Directive**: Enhance EU cybersecurity, addressing increasing sophisticated and frequent cyber threats.
- **Background**: Response to escalated cyber-attacks on essential services (healthcare, finance, energy, transport).
- **Limitations of Original NIS Directive**: Limited scope and varied implementation across EU member states.
- **Key Features of NIS 2 Directive**:
  - Expanded regulatory scope to include more sectors and digital services.
  - Mandatory risk management and incident reporting for public administrations and medium to large entities in critical sectors.
- https://www.nis-2-directive.com/

NIS 2 Directive – Goals & Applicability

MAIN GOALS

- Require national governments to pay due attention to cybersecurity
- Strengthen European cooperation among cybersecurity authorities
- Require the main operators in key industries of our society to take security measures and report incidents.

APPLIES TO ENTITIES IN SECTORS OF HIGH CRITICALITY

- A large entity is defined as a company with at least 250 employees OR with an annual turnover of at least 50 million euros or an annual balance sheet total of at least 43 million euros
- A medium-sized enterprise is defined as one with at least 50 employees OR with an annual turnover (or balance sheet total) of at least 10 million euros
- Estimated 160,000 companies affected by NIS 2

IMPLEMENTATION DEADLINE

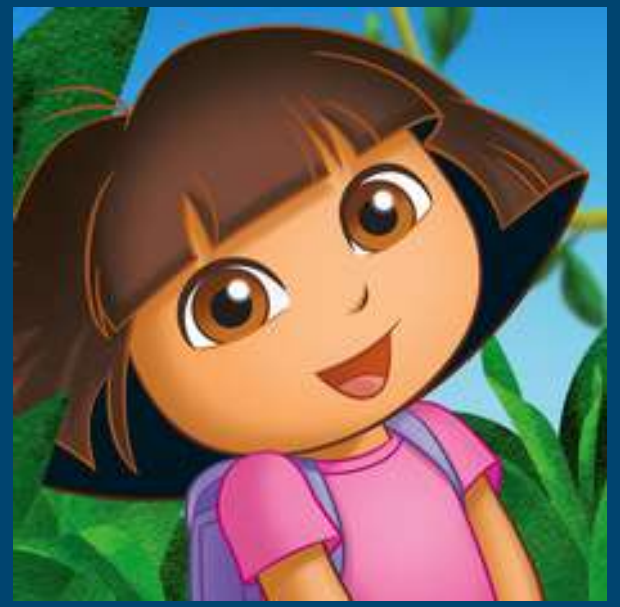
- October 17, 2024

NIS 2 and what it means to F5

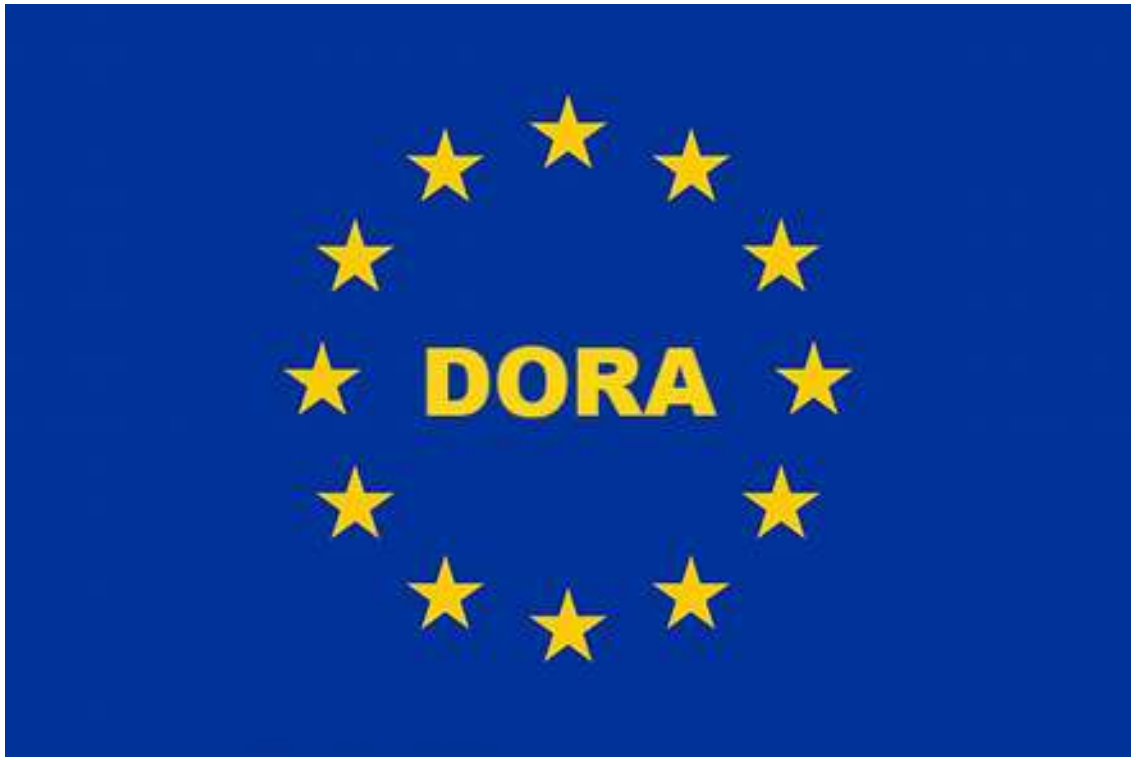
Opportunities and talking points

- NIS 2 includes stricter security requirements and addresses a **wider range of businesses** and sectors
  => Enhances cybersecurity awareness and interest across a wide range of industries
- Experts estimate that roughly **150,000 entities** across the EU are affected by NIS 2
  => Expanded market opportunity for advanced cybersecurity solutions
- Many of these medium sized organization will not have the **skills nor resources** to manage all this complexity
  => Opportunity for SaaS-based and managed services (through channel/MSP) offerings through F5 Distributed Cloud
- **Reporting obligations** (with severe penalties for non-compliance) require visibility into attacks
  => F5 Distributed Cloud centralized visibility + export to SIEM/SOAR platforms
- Specific requirements on **cryptography**
  => Position F5 as established leader in SSL offload, position SSL-O solutions and elevate discussion to post-quantum crypto

DORA
Digital Operational Resilience Act



Introduction to DORA



The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will **apply as of 17 January 2025**.

Aims at **strengthening the IT security of financial entities** such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonization of the rules relating to **operational resilience for the financial sector** applying to 20 different types of financial entities and ICT third-party service providers.

https://www.dora-info.eu/

Main elements of DORA – What does it cover ?

ICT Risk Management Framework

Financial Entities must have a resilient ICT risk management system in place, including a **business continuity** policy and a **disaster recovery** procedure

Classification and Reporting of ICT-related Incidents

Financial Entities must implement an ICT-related incident management process, including early warning indicators, to detect, manage and notify ICT-related incidents creating a consistent **incident reporting** mechanism

Resilience Testing of ICT Tools and Systems

Financial Entities must establish a comprehensive digital operational resilience testing programme. Some Financial Entities are required to test their ICT tools, systems and processes at least every three years using **penetration tests**

Third Party Risk Management

Financial Entities must manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework. This entails that, among other things, the contracts governing the relationship will be required to contain certain contractual elements, such as: an indication of locations where data is to be processed and a description of services and guarantees for access, recovery and return in case of failures.

Threat Information Sharing

DORA contains provisions which facilitate the information sharing by Financial Entities of cyber threat information and intelligence, including tactics, techniques, procedures and cyber security alerts to enhance the digital operational resilience across the sector.

Risk Management – Art. 9 : Protection & Prevention

ICT solutions and processes shall:

- ensure the security of the means of transfer of data;
  => Encryption / SSL
- minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity
  => Access / ZTNA
- prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;
  => DDOS, WAF

Risk Management – Art. 10 : Detection

Financial entities shall

- have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.
  => end-to-end visibility tools (F5 XC Console)
- shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.
  => end-to-end visibility tools (F5 XC Console)

Digital Operations Resilience testing – Art. 25 : Testing of ICT tools

- The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

  => vulnerability assessment and pen testing (F5XC Web App Scanning)

DORA and what it means to F5

Opportunities and talking points

- DORA includes stricter security requirements for finance sector and **broadens scope** to insurance sector, crypto companies, etc
  => Enhances cybersecurity posture of all these companies which represents a business opportunity for us
- **Reporting obligations** (with severe penalties for non-compliance) require visibility into attacks
  => F5 Distributed Cloud Console - Centralized visibility & export to SIEM/SOAR
- Operational resilience will drive **multi-cloud** adoption (single cloud is unlikely to be accepted by auditors) and **multi-vendor** security vendor strategy
  => Opportunity to position our multi-cloud capabilities (consistent security policies + secure MCN for cloud migration/resiliency)
  => Second vendor position (addressing Akamai incumbency)
- Specific requirements on **vulnerability assessments and scans (Art. 25)**
  => Opportunity to introduce F5 Distributed Cloud Web App Scanning (HeyHack)
- DORA puts **requirements on 3rd party ICT service providers** as well, so F5 may be subject to specific contractual conditions and/or requirements.
  => Our legal teams are investigating this through our external auditors, but so far no obstacles have been identified

AI Act
Artificial Intelligence Act

Introduction to AI Act

The AI Act is the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally.

The AI Act ensures that AI systems are safe and transparent and that consumers in the EU are not exposed to risks.

The EU AI Act legislative text therefore pursues a risk-based approach to the regulation of AI systems and classifies the A.I. systems into four different categories:

- unacceptable risk, high risk, limited risk, low risk

https://artificialintelligenceact.eu/

High risk AI providers must …

- Establish a **risk management system** throughout the high risk AI system's lifecycle;
- Conduct **data governance**, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.
- Draw up **technical documentation** to demonstrate compliance and provide authorities with the information to assess that compliance.
- Design their high risk AI system for **record-keeping** to enable it to automatically record events relevant for identifying national level risks and substantial modifications throughout the system's lifecycle.
- Provide **instructions for use** to downstream deployers to enable the latter's compliance.
- Design their high risk AI system to allow deployers to implement **human oversight**.
- Design their high risk AI system to achieve appropriate levels of **accuracy, robustness, and cybersecurity**.
- Establish a **quality management system** to ensure compliance.

All providers of GPAI models must …

- Draw up **technical documentation**, including training and testing process and evaluation results.
- Draw up **information and documentation to supply to downstream providers** that intend to integrate the GPAI model into their own AI system in order that the latter understands capabilities and limitations and is enabled to comply.
- Establish a policy to **respect the Copyright Directive**.
- Publish a **sufficiently detailed summary about the content used for training** the GPAI model.
- Perform **model evaluations**, including conducting and documenting **adversarial testing** to identify and mitigate systemic risk.
- **Assess and mitigate possible systemic risks**, including their sources.
- **Track, document and report serious incidents** and possible corrective measures to the AI Office and relevant national competent authorities without undue delay.
- Ensure an adequate level of **cybersecurity protection**.

Summary

Summary

NIS 2 (160,000 companies impacted)

- Opportunity for F5 Distributed Cloud as many (smaller) companies will have to increase their efforts in cybersecurity
- Many organizations will lack skills and resources : SaaS offering or managed service (through our MSP partners)
- Reporting obligations : F5 Distributed Cloud Console
- Requirements on cryptography : open a discussion on SSL offload, post-quantum crypto

DORA (22,000 companies impacted)

- Reporting obligations : F5 Distributed Cloud Console
- Operational resilience will drive multi-cloud adoption and multi-vendor strategies
- Vulnerability assessment and penetration testing mandatory every year : F5 Distributed Cloud Web App Scanning

AI Act