



ATHEXGROUP

Your Trusted Partner for

Sustainable Cyber Resilience

Greece | Cyprus | Belgium | Romania | United States

Strategies for Achieving PSD3, DORA, and NIS2 Compliance

Mustafa SICAK
GRC & Cyber Security Advisor

Cybersecurity in Greek Financial Institutions - 2025



~757
Average weekly
cyberattacks per bank

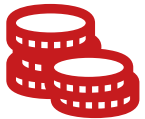
+17% YoY, ~1,612
Overall cyberattacks
(all sectors)

EU finance distribution, mirrored in Greece
DDoS **83%** Data breach **9,5%** Ransomware **5.3%**

69%
Bank targeted of
finance incidents

4.7%
Financial sector share of
all EU cyber incidents

EU Ransomware strains
Akira, Datacarry, BlackLock

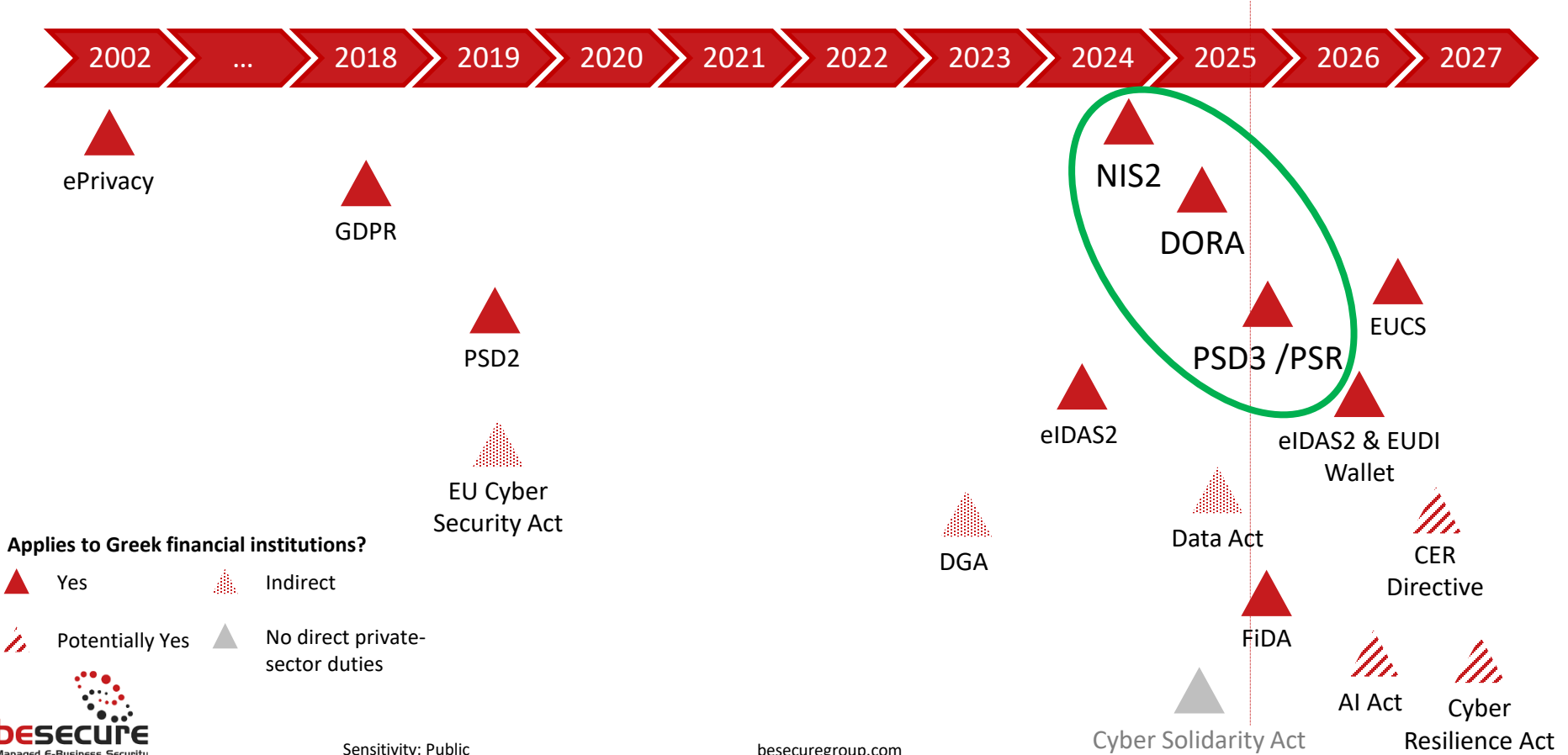


€220,000
GDPR fine
Greek Bank

€100,000
GDPR fine
Greek bank

€50,000
GDPR fine
Greek Bank

EU Regulations overview – Cyber Security & Privacy



Focus on DORA, NIS2 and PSD3



Regulation (EU) 2022/2554
Greek Law: 5193/2025

- Operational resilience & ICT risk**
- Detailed, prescriptive
- Supervisor: Bank of Greece, HCMC
- Penalties:
 - Legal entities: <2% annual global turnover
 - Senior Manager: up to <€1M
 - ICT providers: < 1% average daily global turnover or daily fines up to 6 months



Directive (EU) 2022/2555 *
Greek Law: 5160/2024

- Baseline cybersecurity maturity**
- Broad, principle-based
- Supervisor: National Cyber Security Authority
- Penalties:
 - Legal entities: <€10M or <2% annual global turnover



Still EU proposals
Greek Law: not transposed yet

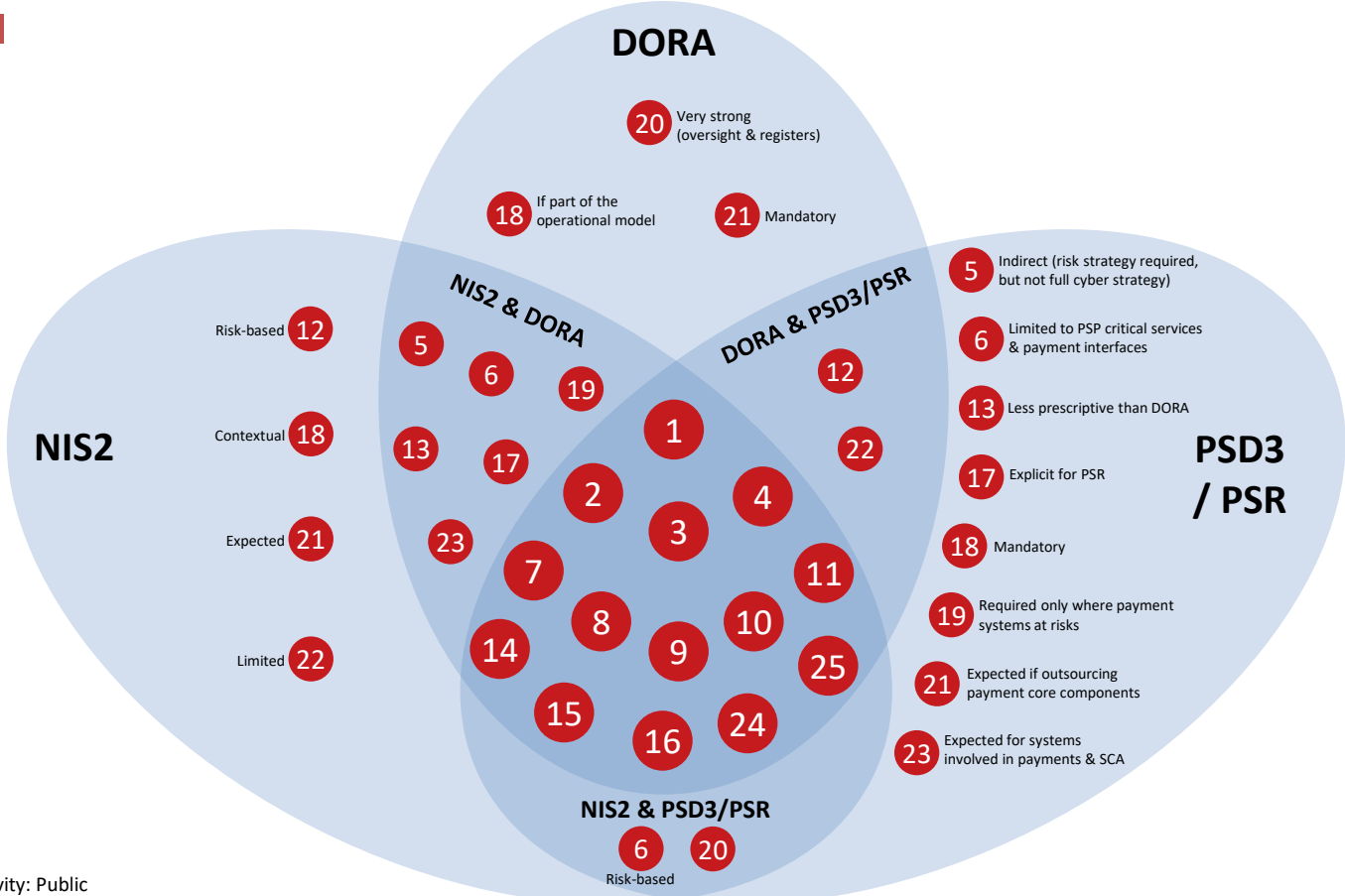
- Payment security & Fraud prevention**
- Technical & consumer-protection driven
- Supervisor Bank of Greece
- Penalties:
 - Legal entities: at least 10% of annual turnover
 - Individuals: at least €5m
 - Risk of significant fines, revocation of License and public censure

* For financial institutions, where DORA applies in detail, DORA takes precedence (lex specialis). NIS2 still influences national coordination and critical infrastructure designation.

Focus on DORA, NIS2 and PSD3

Security Controls

- 1 Cybersecurity Governance & Roles
- 2 Board-Level Accountability for ICT & Fraud Risk
- 3 Information Security Policy Framework
- 4 Risk Management Framework
- 5 ICT & Cybersecurity Strategy
- 6 Asset Inventory (IT, Data, Services)
- 7 Logging & Monitoring
- 8 Security Incident Detection & Response
- 9 Incident Reporting to Authorities
- 10 Business Continuity Management (BCM)
- 11 Disaster Recovery & Resilience Testing
- 12 Penetration Testing / Red Teaming
- 13 Vulnerability & Patch Management
- 14 Change & Configuration Management
- 15 Identity & Access Management (IAM)
- 16 Strong Customer Authentication (SCA)
- 17 Cryptographic Controls / Secure Channels
- 18 Transaction Fraud Detection & Anomaly Monitoring
- 19 Network Segmentation / Boundary Defense
- 20 Supply Chain / ICT Third-Party Risk
- 21 Outsourcing Register
- 22 Operational Resilience Testing Program
- 23 Secure Software Development Lifecycle (SSDLC)
- 24 Data Protection / GDPR Alignment
- 25 Security Training & Awareness



It is time to BeSecure

Our mission: we serve as a **strategic partner**, simplifying the **compliance journey** and **minimising operational burden** of our clients.

We deliver a **unified governance and compliance framework** to ensure consistent alignment with regulatory and industry requirements across the organization.

Our **operational resilience and cybersecurity model** is continuously optimized to anticipate and mitigate emerging threats.

We provide **strategic C-level advisory** that strengthens decision-making, supports prioritisation, and ensures effective oversight of digital and cyber risk.

We offer a **broad and integrated suite of services**, covering:



Governance, Risk & Compliance (*including tooling*)



Security Assurance (*Audit, Assessment, pentesting etc*)



Cyber Security solutions

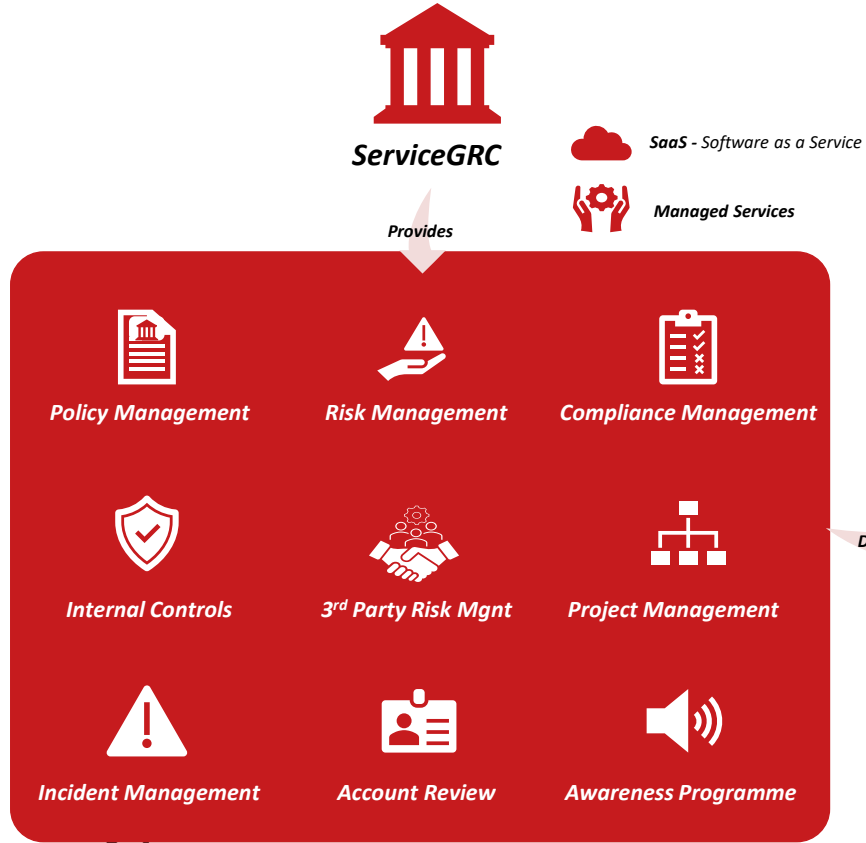


Managed Security Services



Certification Training & Awareness programs

Use-case 1: Unified Governance Risk and Compliance



Success Story: Leading SaaS provider for global airlines
Worldwide Electronic Money Transfer Institution

- Regulatory Assurance**
 - ✓ **60 - 80% less time** spent on compliance reporting.
 - ✓ **50% fewer audit findings** and strong reduction in regulatory fine exposure (up to **€10M+** under NIS2/DORA).
- Significant Cost Reduction**
 - ✓ **25 - 40% OPEX savings** in compliance operations.
 - ✓ **30 - 50% lower audit and advisory costs.**
 - ✓ Savings: **€500k - €1.2M/year** for a mid-sized bank.
- Enhanced Cyber & Operational Resilience**
 - ✓ **40 - 60% faster incident detection/response.**
 - ✓ **15 - 30% fewer service disruptions**, reducing downtime (costs **€30k - €70k per hour**).
- Efficient Third-Party Risk Management (DORA)**
 - ✓ **50% faster vendor assessments.**
 - ✓ **30 - 40% less effort** on outsourcing governance.
 - ✓ Savings: **€100k - €200k/year.**
- Faster, Predictable Compliance for New Regulations**
 - ✓ **50% faster adoption** of new EU regulations.
 - ✓ Avoids last-minute remediation costs (**€500k - €2M** per regulation).
- Better Risk Visibility for Executives**
 - ✓ **Up to 15% reduction in operational losses** through improved controls.

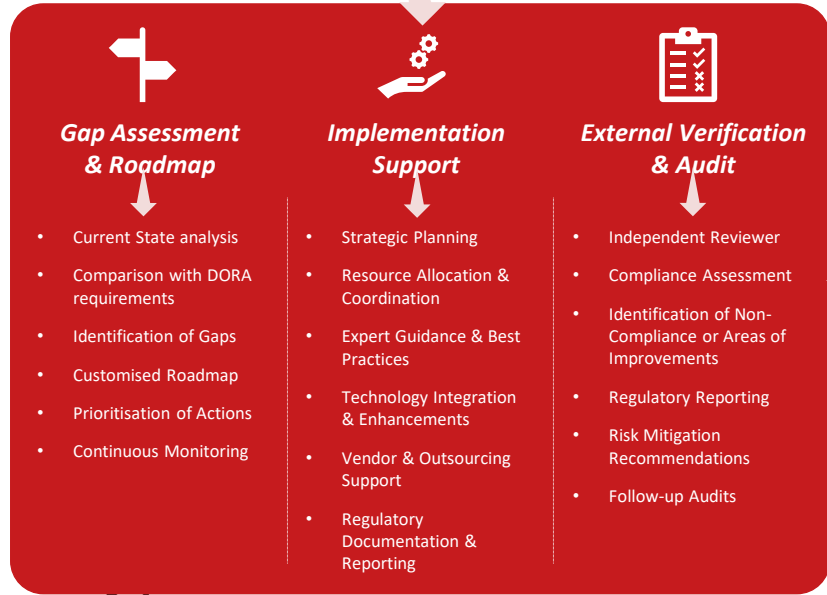
Use-case 2: Compliancy Assurance Services



Robust Approach



Provides



Success Story:

Numerous enterprises in Greece, Cyprus and Belgium

- ✓ Accelerate NIS2 and DORA compliance by 40 - 60%
- ✓ Cut compliance OPEX by 25 - 40%
- ✓ Reduce audit findings by 50%
- ✓ Minimize downtime and ICT disruptions by 15 - 30%
- ✓ Lower regulatory risk exposure fines up to €10M
- ✓ Reduce vendor and outsourcing risks by 30 - 40%
- ✓ Annual financial benefits by €1.2M - €4.6M
- ✓ Regulatory fine exposure reduced by €10M+

Use-case 3: Customer Digital Onboarding



Digital Onboarding

Provides



SaaS - Software as a Service



Managed Services

Success Story: Global Financial Services Provider achieving secure and cost-effective digital onboarding of millions of customers.

Secure self-service identity verification using smartphone

- trust the user
- trust the device
- provision a credential

Establish Trust



- secure access
- secure transactions
- sign transactions

Transact



Monitor:

- user behavior
- session activity
- system wide patterns

Maintain Trust

Delivers

- ✓ **Remove regulatory complexity** across DORA, NIS2, PSD3/PSR
- ✓ **Faster, secure digital onboarding** by 60 - 80%
- ✓ **Reduction in compliance workload** by 50 - 70%
- ✓ **Lower onboarding & verification costs** by 30 - 50%
- ✓ **Reduction in onboarding and identity fraud** by 60 -80%
- ✓ **Fewer audit findings** by 50%
- ✓ **Fewer ICT disruptions (reduces downtime cost)** by 15 -30%
- ✓ **Annual financial benefit €1.5M - €5M**
- ✓ **Regulatory fine exposure reduced** by €10M+



Capture & Classify:

World class patented image capture that automatically crops & detects document type, region & prevents glare, in compliance with PRADO



Facial Recognition:

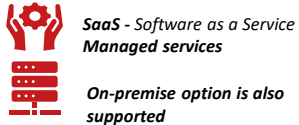
Two classes of facial recognition match and liveness tests



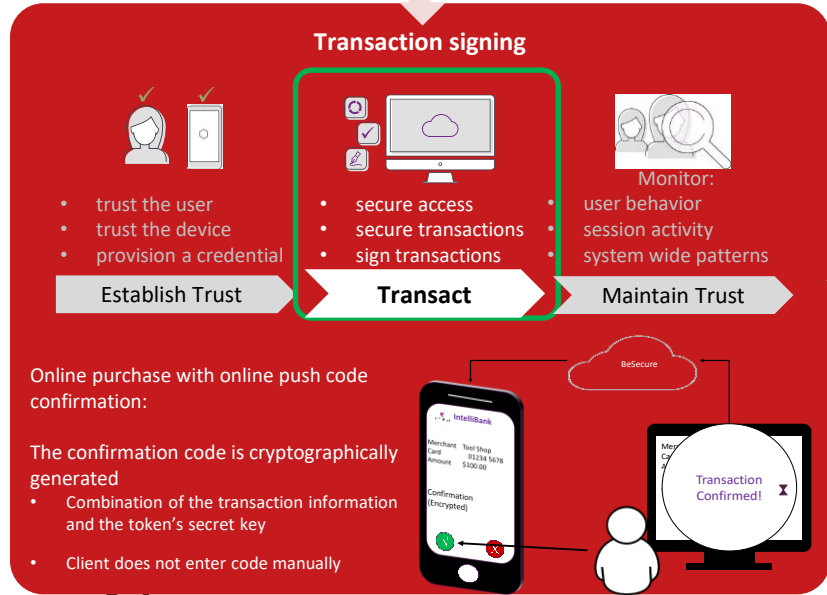
Authentication

Accurate data population with 50+ forensic tests run in seconds in the same seamless process

Use-case 4: Financial Transactions Signing



Success Story: Leading Greek Financial Institution, protecting the financial transactions of millions of customers against daily frauds



- ✓ **Remove regulatory complexity** with DORA, NIS2, PSD3/PSR
- ✓ **Reduction in fraud & unauthorized transactions** by 50 - 80%
- ✓ **Faster digital signing processes** by 60 - 80%
- ✓ **Fewer authentication-related incidents** by 40 - 60%
- ✓ **Lower compliance OPEX** by 25 - 40%
- ✓ **Fewer audit findings** by 50%
- ✓ **Fewer operational errors** by 20 - 40%
- ✓ **Annual financial benefits** by €1.8M - €5.5M
- ✓ **Regulatory & fraud risk avoidance** by €10M+

Use-case 5: Mobile Application Shielding



Mobile App Security



Enterprise Security Solution

Provides

Protect Mobile Application Lifecycle



Security Testing

- Actionable recommendations to fix security issues
- Address security bugs early
- Code optimisation
- Secure code, APIs, and cryptography



Multi-layer Security

- Encryption, obfuscation
- Mobile apps and API hardening
- Runtime Application Self-Protection (RASP)
- Anti-tamper enforcement



Real-time Threat monitoring

- Detect threats in real time
- Get actionable insights
- Adjust security protection strategy accordingly

Delivers

Success Story: European Financial Institution, safeguarding the savings of millions of depositors.

- ✓ Remove regulatory complexity with DORA, NIS2, PSD3/PSR
- ✓ Reduction in mobile fraud and tampering by 50 - 80%
- ✓ Fewer mobile-related security incidents by 30 - 50%
- ✓ Fewer exploitation attempts on the mobile channel by 60 - 70%
- ✓ Lower compliance and development costs by 25 - 40%
- ✓ Reduction in ICT disruptions 20 - 30%
- ✓ Annual financial benefits by €1.5M - €5M
- ✓ Avoided regulatory and fraud exposure by €10M+
- ✓ Faster, safer mobile banking leads to higher customer trust



ATHEXGROUP

Your Trusted Partner for

**Sustainable
Cyber Resilience**

Message for Executives

What is YOUR need?

Greece | Cyprus | Belgium | Romania | United States



Thank You!

Mustafa Sicak
GRC & Cyber Security Advisor
m.sicak@besecure.io

EU Regulations overview

Regulation	What it covers (very short)	Applies to Greek financial institutions?	Dates
GDPR — Regulation (EU) 2016/679	EU-wide personal data protection & breach notification.	Yes, fully. Controllers/processors incl. banks, insurers, FMIs, PSPs.	Applies since 25 May 2018
ePrivacy — Directive 2002/58/EC (as amended by 2009/136/EC)	Privacy in electronic communications; cookies/consent; spam.	Yes, for channels & cookies. Applies via Greek transposition to websites/apps/communications used by banks.	In force since 2002; cookie consent strengthened 2009; ongoing under national law until any future ePrivacy Regulation.
DORA — Regulation (EU) 2022/2554 (+ Dir. (EU) 2022/2556)	ICT risk mgmt, incident reporting, testing, 3rd-party risk, threat-led testing for the financial sector.	Yes, core regime for banks/insurers/investment firms/PSPs/FMIs in Greece.	Applies from 17 Jan 2025 (RTS/ITS phased; ESA standards accompany)
NIS2 — Directive (EU) 2022/2555	Baseline cybersecurity & incident reporting for essential/important entities.	Generally yes, but for financial entities DORA is lex specialis (NIS2 can still apply to uncovered aspects under Greek law).	Member-state transposition by 17 Oct 2024; national measures apply from 18 Oct 2024 (Greece has transposed)
EU Cybersecurity Act — Regulation (EU) 2019/881	ENISA's permanent mandate; EU cybersecurity certification framework (EUCC, EUCS, etc.).	Indirect. No day-to-day duties for banks unless using/asking for certified products; relevant for supplier assurance.	In force/applicable from 27 Jun 2019; certification schemes roll out via implementing acts (e.g., EUCC 2024)
Cyber Resilience Act (CRA) — Regulation (EU) 2024/2847	Security-by-design & vuln. mgmt for products with digital elements; CE marking.	Only if you place products on the market. As product users, banks feel it via procurement.	In force 10 Dec 2024; main obligations apply 11 Dec 2027 (some earlier milestones)
eIDAS & eIDAS 2 — Regulation (EU) 910/2014, amended by 2024/1183	EU digital identity wallets; qualified trust services & remote signing.	Practically yes. Banks will need to accept EUDI Wallet credentials where required once implementing acts land.	Amendment adopted 20 May 2024; wallets delivered within ~24 months of implementing acts
Data Governance Act (DGA) — Regulation (EU) 2022/868	Data intermediaries, data altruism, reuse of protected public-sector data.	Indirect. Only if acting as data intermediary or reusing protected public data.	In force 23 Jun 2022; applicable since 24 Sept 2023.
Data Act — Regulation (EU) 2023/2854	Access/use of IoT & other data; cloud switching & interoperability; B2B/B2G access.	Indirect but common. Affects banks as data users/holders and major cloud customers.	Applicable from 12 Sept 2025 (staggered duties).
PSD2 SCA RTS — Commission Delegated Regulation (EU) 2018/389	Strong Customer Authentication & secure communications for payments.	Yes (PSPs). Greek banks/PSPs must perform SCA & support secure APIs.	Applies from 14 Sept 2019 (some card e-commerce had phased national migrations).
AI Act — Regulation (EU) 2024/1689	Risk-based AI controls, incl. governance, robustness & cybersecurity for AI (e.g., credit scoring, fraud).	Likely yes if you develop/deploy AI systems (incl. high-risk).	In force 1 Aug 2024; bans & literacy from 2 Feb 2025; most rules from 2 Aug 2026; some to 2027.
Cyber Solidarity Act — Regulation (EU) 2025/38	EU-level alert system, cyber reserve, emergency mechanism.	No direct private-sector duties; affects cross-border response that can involve finance.	Applies from 4 Feb 2025
CER Directive — Directive (EU) 2022/2557 (Critical Entities Resilience)	Physical/operational resilience of critical entities (incl. banking & FMI).	Potentially yes. Applies if a Greek bank/FMI is designated a critical entity (separate from cybersecurity).	Transpose by 17 Oct 2024; entities identified by 17 Jul 2026, then 10 months to comply (latest May 2027)

Security Controls mapping

	Security Control	NIS2	DORA	PSD3 / PSR (replacing PSD2 SCA RTS)
1	Cybersecurity Governance & Roles	✓ Required	✓ Required (strong governance)	✓ Required (PSP governance strengthened under PSD3)
2	Board-Level Accountability for ICT & Fraud Risk	✓ Required	✓ Strongly Required	✓ Required (explicit in PSD3 supervisory expectations)
3	Information Security Policy Framework	✓ Required	✓ Required	✓ Required for PSPs (PSR risk & fraud policies)
4	Risk Management Framework	✓ Required	✓ Required	✓ Required (enhanced fraud risk & transaction risk assessment)
5	ICT & Cybersecurity Strategy	✓ Required	✓ Required (mandatory)	● Indirect (risk strategy required, but not full cyber strategy)
6	Asset Inventory (IT, Data, Services)	✓ Required	✓ Required	● Limited to PSP critical services & payment interfaces
7	Logging & Monitoring	✓ Required	✓ Required	✓ Required for transaction & fraud monitoring under PSR
8	Security Incident Detection & Response	✓ Required	✓ Required	✓ Required (fraud + operational, reportable to NCA)
9	Incident Reporting to Authorities	✓ Required	✓ Required (financial supervisors + ESAs)	✓ Required (fraud/operational incidents under PSR)
10	Business Continuity Management (BCM)	✓ Required	✓ Required (tested, documented)	✓ Required (PSR continuity obligations for PSPs)
11	Disaster Recovery & Resilience Testing	✓ Required	✓ Required (evidence & testing cycles)	✓ Required (PSR mandates DR/continuity for PSP infrastructure)
12	Penetration Testing / Red Teaming	✓ Risk-based	✓ Required (incl. TLPT for critical entities)	✓ Required (risk-based security testing for PSPs)
13	Vulnerability & Patch Management	✓ Required	✓ Required	✓ Required but less prescriptive than DORA
14	Change & Configuration Management	✓ Required	✓ Required	✓ Required for PSP systems handling transactions
15	Identity & Access Management (IAM)	✓ Required	✓ Required	✓ Required (SCA reinforces IAM governance)
16	Strong Customer Authentication (SCA)	● Only for high-risk sectors	✓ If internal risk model demands	✓ Central requirement under PSR (continuation + tightening of PSD2 SCA)
17	Cryptographic Controls / Secure Channels	✓ Required	✓ Required	✓ Explicit for PSR: payment channel integrity + dynamic linking
18	Transaction Fraud Detection & Anomaly Monitoring	● Contextual	● If part of operational model	✓ Mandatory (fraud analytics & behavioural monitoring enhanced)
19	Network Segmentation / Boundary Defense	✓ Required	✓ Required	● Required only where payment systems at risk
20	Supply Chain / ICT Third-Party Risk	✓ Required	✓ Very strong (ICT TPP oversight & registers)	✓ Required (PSPs must ensure SCA & security controls extend to third parties)
21	Outsourcing Register	● Expected	✓ Mandatory under DORA	● Expected if outsourcing payment core components
22	Operational Resilience Testing Program	● Limited	✓ Fully Required (scenario, TLPT, DR)	✓ Required for PSP continuity & fraud mitigation effectiveness
23	Secure Software Development Lifecycle (SSDLC)	✓ Required	✓ Required	✓ Expected for systems involved in payments & SCA
24	Data Protection / GDPR Alignment	✓ Required	✓ Required	✓ Required (customer data & transaction metadata)
25	Security Training & Awareness	✓ Required	✓ Required	✓ Required (fraud reduction & PSP staff training)

DORA Overview

To ensure that the **entire financial sector** can **withstand, respond to, and recover** from **ICT-related** disruptions and cyber threats.

1 Scope & Definitions

- Financial entities (banks, insurers, investment firms, PSPs, FMIs, ICT third-party providers)
- ICT-related incident definition

2 ICT Risk Management Requirements

- Governance (board accountability)
- ICT risk framework & policies
- Asset management (ICT inventory)
- Logging, monitoring, alerting
- Access management & system security
- Backup, disaster recovery, continuity

3 ICT-Related Incident Management & Reporting

- Incident classification criteria
- Reporting timelines to supervisor
- Post-incident analysis requirements

4 Digital Operational Resilience Testing

- Periodic vulnerability testing
- Threat-led penetration testing (TLPT) for significant entities
- Test remediation validation

5 ICT Third-Party & Outsourcing Risk

- Outsourcing registers
- ICT service contract controls
- Critical providers under direct ESMA/EBA/EIOPA oversight

6 Information Sharing Arrangements

- Sector-wide cyber threat intelligence sharing encouraged

7 Supervision, Enforcement & Penalties

NIS2 Overview

To raise cybersecurity maturity and resilience across **critical sectors**, including energy, transport, health, digital infrastructure, **and finance** (unless covered by DORA in overlapping area).

1 Scope & Entity Classification

- Essential Entities (high criticality)
- Important Entities (lower criticality tier)

2 Governance & Accountability

- Management body holds direct responsibility
- Mandatory cybersecurity risk management measures

3 Cybersecurity Risk Management Requirements

- Policies for risk assessment & security controls
- Incident handling & prevention
- Encryption & secure communications
- Supply chain / vendor cybersecurity controls
- Secure development & vulnerability management

4 Incident Reporting

- Early warning → incident notification → final report
- Deadlines (usually within 24–72 hours depending on severity)
- Coordination with national CSIRT

5 Supervision & Enforcement

- Audits, inspections, penalties

6 Cross-Border Cooperation

- Cooperation via European Cyber Crises Liaison Organization Network (EU-CyCLONE)

For financial institutions, where DORA applies in detail, DORA takes precedence (lex specialis). NIS2 still influences national coordination and critical infrastructure designation.

PSD3 & PSR Overview

PSD3 = Directive on licensing, governance & supervision
PSR (Payment Services Regulation) = Regulation for technical and operational rules, including SCA & anti-fraud

To strengthen **payment security, fraud prevention, consumer protection**, and level competition across payment service providers.

1 Scope & Definitions

- PSPs, payment institutions, EMIs, account information services

2 Licensing & Prudential Requirements (PSD3)

- Authorization rules
- Capital & safeguarding requirements
- Governance & fitness criteria

3 Operational & Security Requirements (PSR)

- Strong Customer Authentication (SCA) requirements
- Secure communications & API standards
- Transaction monitoring & fraud analytics
- Protection against social engineering fraud

4 Consumer Rights & Transparency

- Payment execution timelines
- Complaint handling
- Clearer dispute and liability rules

5 Fraud Prevention Measures

- Mandatory real-time anomaly detection
- Confirmation of Payee system (IBAN/name match)
- Shared fraud data exchange mechanisms

6 Supervision & Enforcement

- National supervisors (e.g., Bank of Greece)
- EU-level monitoring for systemic payment risks