yubico

DORA COMPLIANCE EBOOK

Prepare for DORA Compliance with the YubiKey

European Supervisory Authorities (ESAs) / Lead Overseers:

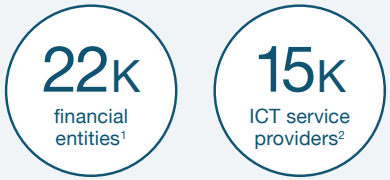
eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Entered force on 16 January 2023 | 17 January 2025 DORA oversight begins

Impacts approximately:



Penalties for non-compliance may be conferred upon:

- Financial entities
- Individuals held responsible
- Members of the management board
- Critical third-party service providers (CTPPs)

Nearly one-fifth of all global cyber attacks in the past 20 years have targeted the financial sector.[3] While the average cost of a cyber attack (€0.45 million) or data breach (€5.53 million) is not likely to cause insolvency, the risk of extreme losses (as large as €2.27 billion) has increased, threatening the solvency of compromised entities as well as global financial stability.[4]

Technological interdependence, such as the shared reliance on third-party information and communication technology (ICT), further increases the risk of systemic impact across entities, sectors and borders. For example, 8% of global cyber incidents in the financial sector in 2023 could be attributed to the MOVEit zero-day exploit, demonstrating the extensive impact of third-party (supply chain) breaches.[5]

What is DORA?

The Digital Operational Resilience Act (DORA)[6] aims to manage ICT risk within the European financial sector and its associated supply chains, enabling it to withstand, respond to and recover from cyber incidents—ensuring financial stability even in the event of severe operational disruptions.

DORA establishes a comprehensive framework for managing internal and third-party risk. The regulation was designed to reduce regulatory complexity, whilst harmonising and upgrading rules for operational resilience and risk management that may have appeared in previous legislation across the EU.

Who needs to comply with DORA?

DORA is intended to apply to nearly all financial entities and the ICT third-party service providers (TPPs) they rely upon, including cloud service providers, data processors and other ICT services. Covered ICT TPPs may be located anywhere in the world, not just from premises within the European Union.

At the start of 2025, some ICT TPPs will be designated as critical (CTPPs)—those ICT TPPs who support critical or important functions of multiple financial entities and whose failure could have a systemic impact on the stability, continuity or quality of financial services.[7] The ESAs will have direct oversight over CTPPs, requiring that CTPPs establish a subsidiary within the EU and carry the cost of oversight, proportional to turnover.

Financial entities[8]

Credit institutions	Payment institutions	Account information service providers	Electronic money institutions	Investment firms
Crypto-asset service providers	Central securities depositories	Central counterparties	Trading venues	Trade repositories
Alternative investment fund managers	Management companies	Data reporting service providers	Insurance and reinsurance undertakings	Insurance, reinsurance and ancillary insurance intermediaries
Institutions for occupational retirement provision	Credit rating agencies	Critical benchmarks administrators	Crowdfunding service providers	Securitisation repositories

Examples of ICT TPPs[9]

Direct or indirect (subcontractor)

Software and application services (off-the-shelf software or custom development)	Network infrastructure services (excluding telecommunication services)
Data centres	ICT consultancy and managed ICT services
Information security and cybersecurity services	Cloud computing providers
Data analysis and data services (including data entry, data storage, data processing)	Other[10]

What's the penalty for non-compliance?

For CTPPs who have been notified of non-compliance, DORA grants the Overseer the power to compel compliance with a daily penalty payment (for up to six months) of up to 1% of the daily average worldwide turnover from the previous business year.

For financial entities found in breach, competent authorities within each Member State will define and apply "proportionate and dissuasive" administrative penalties and/or criminal penalties. These penalties may be applied to a financial entity, a legal person(s) responsible for the breach and/or to members of the management body.

DORA requirements

DORA establishes requirements for financial entities to maintain the security of network and information systems and support resilience. It does so by establishing requirements across these five pillars:

ICT risk management	ICT incident reporting	Digital operational resilience testing	Information and intelligence sharing	ICT third-party risk TPP | CTPP
Strategies, policies and tools to protect data and ICT assets	Management and reporting of ICT-related incidents	Regular testing proportionate to the size and importance of the entity	Formalised sharing arrangements	Mitigation of third-party risk, through contractual provisions and monitoring

While financial entities will, through contractual provisions, require similar risk management efforts from their ICT service providers to comply with DORA, financial entities ultimately assume responsibility to approve, manage and control the use of ICT services, a move designed to "strengthen accountability" over third-party ICT risk.[11]

DORA requirements for authentication

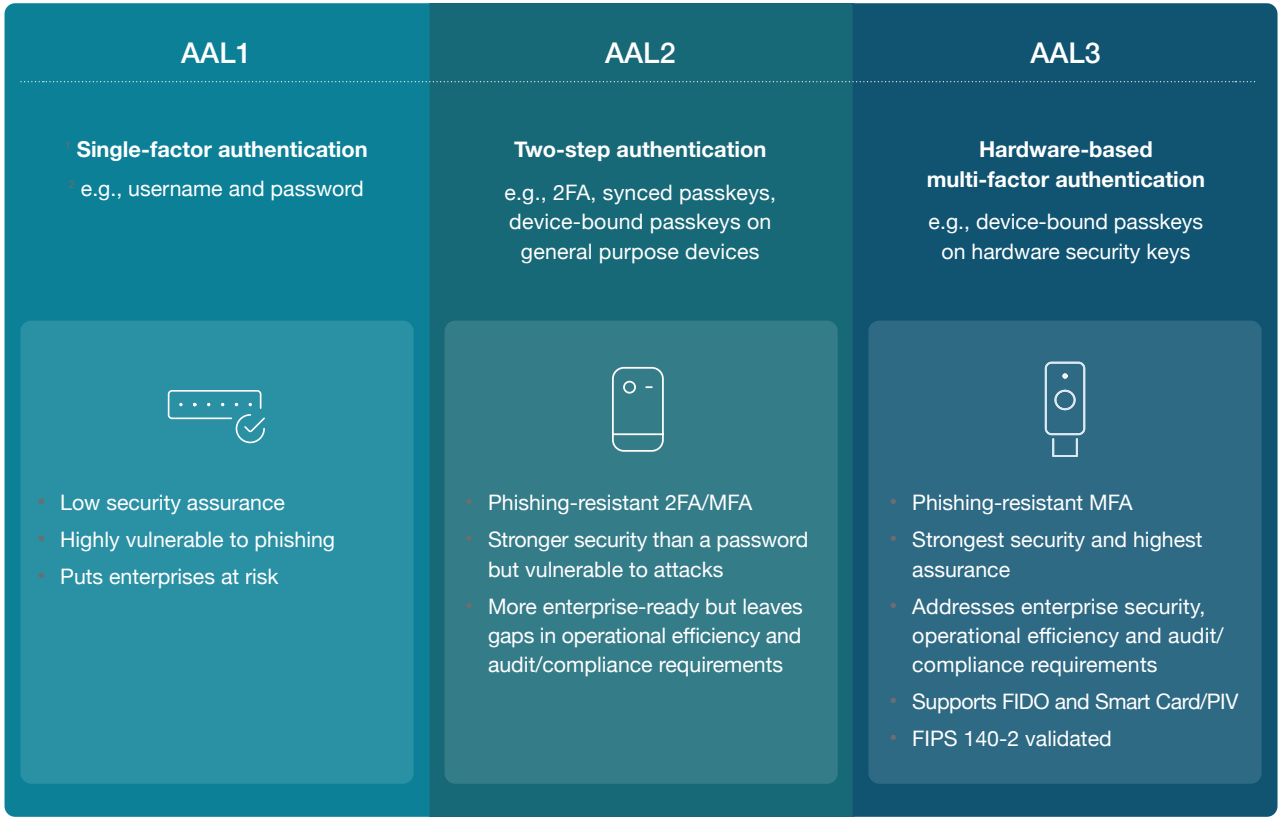
As part of the required risk management framework, covered entities are tasked with establishing “policies and protocols for strong authentication mechanisms” that are “based on relevant standards” and promote “protection measures of cryptographic keys.”[12]

The regulatory technical standards (RTS) designed to support DORA have been designed in line with international standards on ICT risk management, including the Network and Information Security (NIS) Directive, now NIS2, and the NIST Cybersecurity Framework.[13] These standards further clarify that authentication methods should be commensurate to risk and aligned with leading practices for remote access, privileged access and access to critical or important functions.[14]

How to identify authentication risk

To comply with DORA's risk-based authentication requirements, covered entities should select an authenticator based on its strength, referencing the global NIST standard[15] or eIDAS.[16] These guidelines recognize **that not all MFA is created equal,** represented through Authentication Assurance Levels/Levels of Assurance (AALs/LoAs).

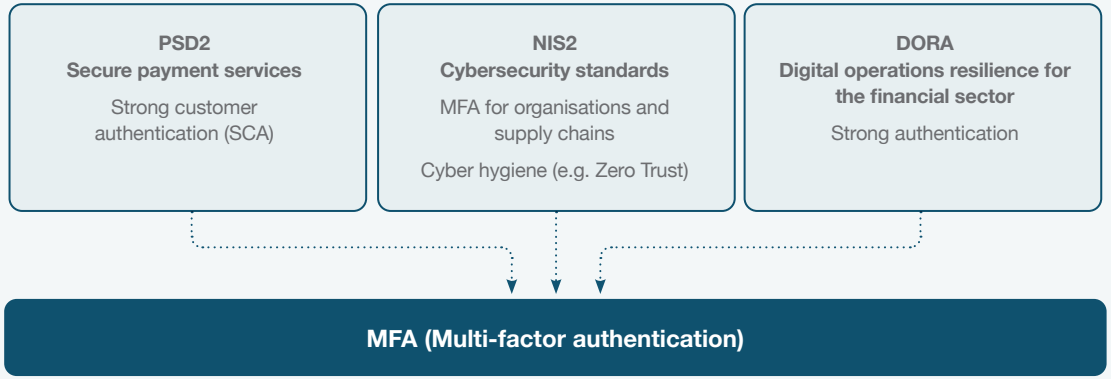
While any form of MFA is better than a password alone (AAL1/LoA Low), legacy forms of MFA (AAL2/LoA substantial) such as SMS, mobile authentication and one-time passcodes (OTP) experience a 10-24% attack penetration rate[17] while a phishing-resistant hardware-based authenticator (AAL3/LoA high) offers higher assurance, reducing the threat of account compromise.[18]



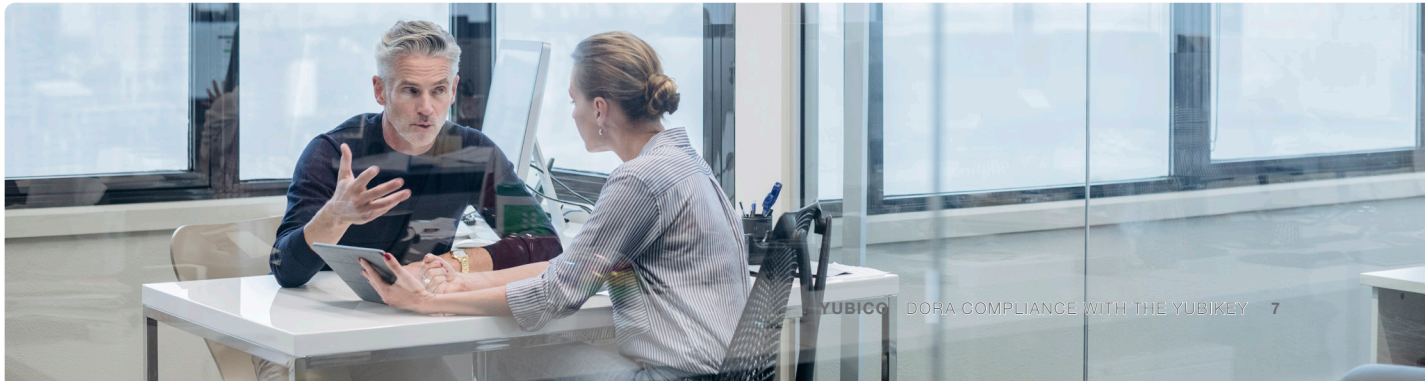
Learn more in our guide to NIS2
Read the guide

How does NIS2 impact DORA?

DORA is a part of a triad of regulations that focus on strengthening digital protections and securing critical digital infrastructure, starting with the consumer and the Payment Services Directive (PSD), now PSD2, and moving toward organisations and their supply chains with DORA and NIS2. All three manage risk with a requirement for strong authentication. Since DORA was designed to align with NIS2, financial organisations—recognised as critical entities—should defer to the more comprehensive requirements of NIS2 including implementing strong MFA (AAL3/LoA high) and Zero Trust principles.



What is critical to note is that while DORA requirements take precedence over NIS2 in areas of overlap, NIS2 requirements continue to apply in other areas.[19] This means that the more specific MFA requirements of NIS2, alongside cyber hygiene practices such as Zero Trust, would suggest that covered entities progress toward the exclusive use of phishing-resistant MFA at AAL2 or higher.



Fast-track DORA compliance with the YubiKey

The YubiKey is a hardware security key built to create organisations of phishing-resistant users. As a hardware root of trust, the YubiKey offers highest-assurance phishing-resistant authentication. Manufactured and programmed in Sweden by Yubico, a Swedish company, the YubiKey is certified against FIPS and FIDO.

Supporting both Smart Card/PIV and FIDO2 protocols, as well as FIDO U2F, OTP/TOTP and OpenPGP, the YubiKey meets you where you are on your cybersecurity journey, and suits a wide range of business scenarios.

- Privileged access
- Mobile restricted
- Shared workstations
- Remote workforce
- Office workers
- 3rd-party access
- End customers

Ensure compliance with DORA requirements by implementing the YubiKey today. For high assurance across your supply chain of ITC TPPs, require that all service providers implement phishing-resistant MFA for their own users and systems.

Contact us
yubi.co/contact

Learn more
yubi.co/finance

Sources

[1] PwC, DORA and its impact on UK financial entities and ICT service providers, (Accessed October 7, 2024)

[2] Joint Committee of the European Supervisory Authorities, ESAs Report on the landscape of ICT third-party providers in the EU, (September 18, 2023)

[3] The International Monetary Fund, Global Financial Stability Report, (April 2024)

[4] Ibid; Verizon, 2024 Data Breach Investigations Report, (May 1, 2024)

[5] Verizon, 2024 Data Breach Investigations Report, (May 1, 2024)

[6] Official Journal of the European Union, REGULATION (EU) 2022/2554, (December 14, 2022)

[7] Joint Committee of the European Supervisory Authorities, JS SC DOR-23-54, (May 26, 2023)

[8] Official Journal of the European Union, REGULATION (EU) 2022/2554, (December 14, 2022)

[9] Joint Committee of the European Supervisory Authorities, ESAs Report on the landscape of ICT third-party providers in the EU, (September 18, 2023)

[10] DORA defines Other ICT Services as: "Digital and data services provided through the ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone service." Official Journal of the European Union, REGULATION (EU) 2022/2554, (December 14, 2022)

[11] Joint Committee of the European Supervisory Authorities, JC 2023 84, (January 17, 2024)

[12] Official Journal of the European Union, REGULATION (EU) 2022/2554, (December 14, 2022)

[13] Joint Committee of the European Supervisory Authorities, JC 2023 86, (January 17, 2024)

[14] Ibid.

[15] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)

[16] European Commission, eIDAS Levels of Assurance (LoA), (2014)

[17] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[18] Office of the European Union, Commission Implementing Regulation (EU) 2015/1502, (September 2015)

[19] Official Journal of the European Union, Commission Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive), (September 18, 2023)

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: www.yubico.com.