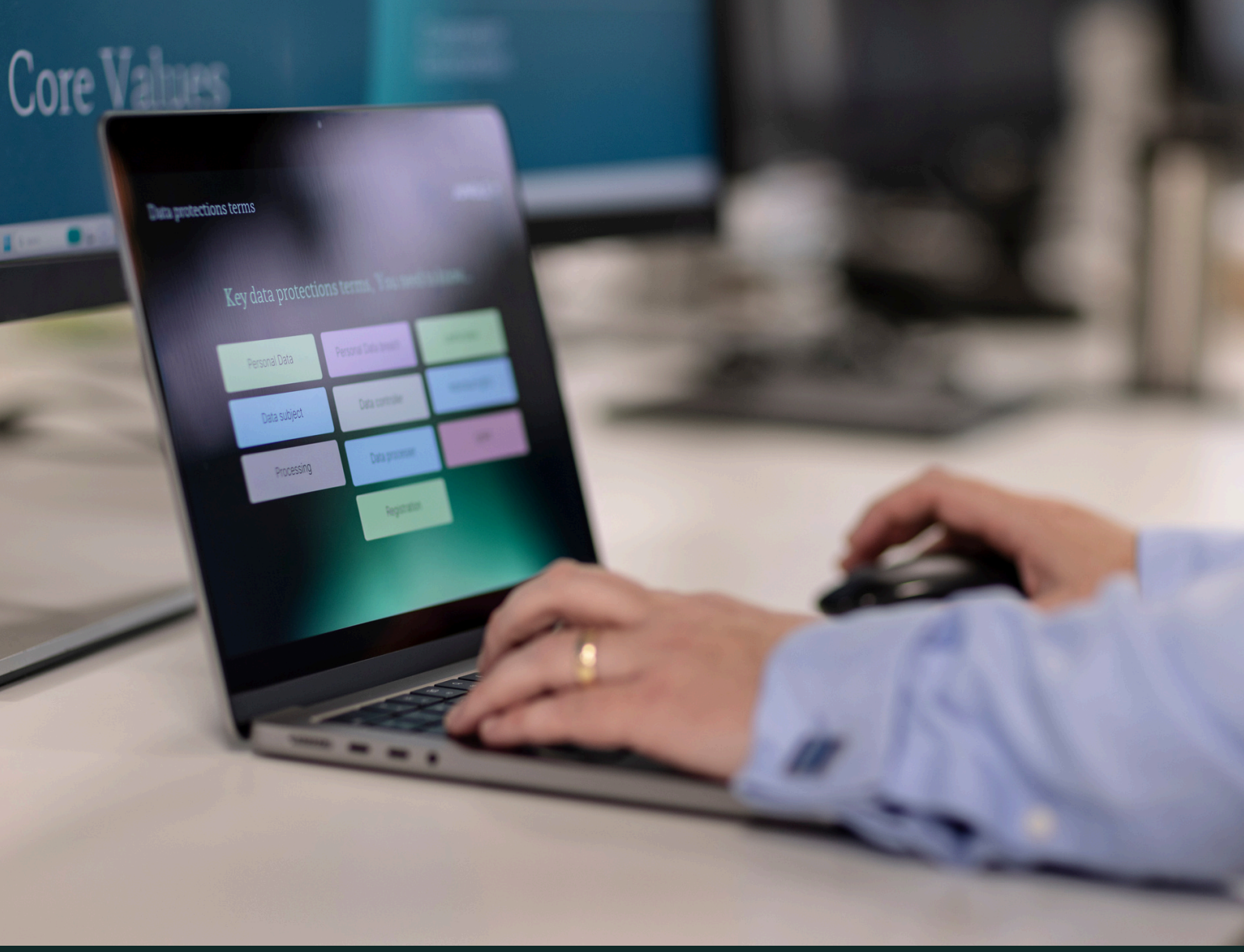



# DORA the exporter: Digital Operational Resilience Act

JUNGLE IT

Exploring the stipulations and implications of DORA on financial businesses

Jungle IT Security Team

hello@jungleit.co.uk
0113 258 4433

jungleit.co.uk

# Contents

# What is the DORA and why is it important?

DORA is the “Digital Operational Resilience Act.”

In simpler terms, DORA documents technical controls and standards that financial companies and third-party technology service providers must implement by January 2025.

Our guide is here to help financial institutions comprehend these changes and make sure their cyber security approach is enhanced.

# Why is DORA a necessity for financial companies?

Digital Operational Resilience Act (DORA) recognises that previous “risk management” for financial institutions primarily focused on “money.” Seeking to answer the question:

**Is the business financially sound?**

DORA recognises that maintaining financial prudence and healthy capital reserves are not sufficient to safeguard financial institutions and European residents from non-financial events.

DORA aims to address not only financial robustness but also technical resilience.

DORA aims to protect companies and those with a financial interest in that company from cyber security threats, not just the unpredictability of subprime mortgages and credit default swaps.

## Who will the Digital Operational Resilience Act (DORA) affect and how?

Even though the Act is an EU regulatory act, with enforcement powers and fines for non-compliance, it will not be enforceable in the UK.

Nevertheless, it will still be important for many UK-based entities as the regulations apply to any financial firms that directly or indirectly, through their group or parent organisation, offer their services in the EU.

As with all things governmental, the DORA regulations establish a benchmark for "indicators of good practice."

Although the specific regulations in the EU Act may not be enforced in the UK, the technical controls they require will start to seep into regulatory bodies, insurance questionnaires, and supply-chain audits.

JUNGLE IT

# Meeting DORA Requirements

The added stipulations for management oversight, executive accountability, risk evaluations, ongoing monitoring, and validation of implemented measures will be integrated into the standard procedures for evaluating a company's governance.

The transition from a focus on "trust" to "trust-but-verify" involves holding CxO level executives personally accountable for ensuring compliance with regulations. This shift is expected to become more standard practice in the business world. Similar to the way Sarbanes-Oxley corporate governance and accounting practices controls found their way into UK regulations.

DORA controls will be seen as best practice and will start to be adopted, if not by government, by regulatory or certification bodies, insurance companies, credit providers, and financial auditors.

# Five DORA pillars explained

DORA has five core pillars covering various aspects of digital operational resilience. These pillars allows for a better understanding of their significance, but will add clarity to enable its practical implementation.

Let's discuss the aspects covered in each of the five pillars.

# Information and Communication Technology (ICT)

### Pillar One: Managing ICT Risks

Financial entities are required to set up a comprehensive ICT risk management framework. This framework details plans to:

- Identify, classify and document critical functions and assets.
- Create and maintain robust ICT systems and tools that reduce the impact of ICT risk.
- Continuously monitor all sources of ICT risks to implement protective and preventative measures.
- Ensure the implementation of robust and all-encompassing business continuity policies, along with thorough disaster recovery plans. Conduct annual testing of these plans to encompass all critical support functions.
- Ensure the set up of systems that can adapt and improve based on external events and the organisation's own technology-related incidents.

### Pillar Two: Reporting ICT incidents

- Devise a streamlined process for logging and classifying all ICT incidents, and determining major incidents on regulatory criteria and specifications from the European Supervisory Authorities (EBA, EIOPA and ESMA).
- To ensure consistency in reporting ICT-related incidents, it is advisable to consolidate standard templates that have been developed by the ESAs.
- Submit an initial, intermediate and final report on ICT-related incidents.

# Information and Communication Technology (ICT)

### Pillar Three: Digital Operational Resilience Testing

The regulation requires all entities to:

- Annually perform basic ICT testing of ICT tools and systems.
- Identify, mitigate and promptly eliminate any weaknesses, deficiencies or gaps regarding ICT issues.
- Periodically perform advanced Threat-Led Penetration Testing (TLPT) for ICT services which impact critical functions. ICT third-party service providers are required to participate and fully cooperate in the testing activities.

### Pillar Four: Managing ICT Third Party Risk

- Diligently monitor risks that could arise from the reliance on technology-related third-party providers.
- Report their comprehensive list of outsourced activities, including intra-group services. Any modifications to the outsourcing of crucial services to third-party ICT service providers should also be included.
- Take account of IT concentrating risk and risks arising from sub-outsourcing activities,
- Enhance the alignment of key service components and the relationship with third-party ICT providers to facilitate comprehensive monitoring.
- Guarantee that the contracts with the ICT third-party providers include all the essential monitoring and accessibility details, such as a comprehensive service level description and indication of locations where data is being processed.
- Critical ICT third-party service providers will be subject to a Union Oversight Framework, which can issue recommendations on the mitigation of identified ICT risks. Financial entities must consider the ICT third-party risks of their service provider who do not follow the defined recommendation.

# Sharing Cyber Security Information

## Creating a cyber security first culture

The importance of sharing cyber security information to raise awareness within your company cannot be overstated.

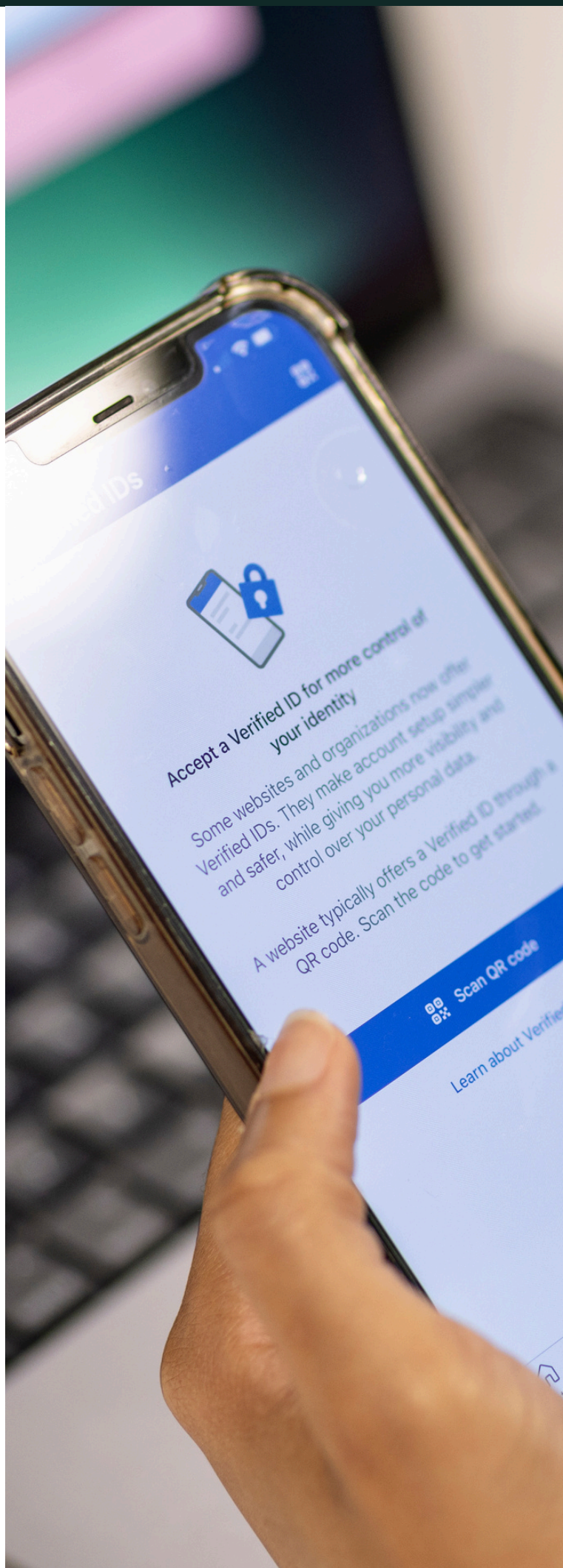
Sharing cyber security information is essential for cultivating a culture of security awareness. When employees are consistently informed about the latest threats, trends, and best practices, they are more equipped to adopt a security-first mindset.

This cultural shift is crucial because it ensures that security is not solely the responsibility of the IT department but is ingrained in the daily operations and awareness of every employee. A security-aware workforce is more vigilant and can serve as the first line of defence against cyber threats.

## Creating a cyber security first culture

By communicating relevant information and ensuring that all employees are aware of their roles and responsibilities, companies can avoid costly fines and legal repercussions.

Regularly sharing updates on regulatory changes and compliance requirements ensures that the organisation remains aligned with industry standards and best practices.



# Beyond DORA

Whilst DORA may not be applicable to your organisation, it highlights areas that clearly need regulating, that can incur fines for non-compliance (up to 1% of last financial years revenue).

It begs the question, why regulate? The answer is that not enough organisations are taking the scale of cyber security incidents seriously enough.

From a technical control perspective, here's key elements to take away:

### Monitor your IT estate

Continually monitor your IT estate. Ensure you know what's going on in your IT environment. Organisations cannot outsource responsibility and accountability to third party IT Service providers.

### Best IT Practices

Adopt IT "best practices" and create a culture of security. People are your best defence, and helping your people become cyber-savvy is essential.

### A Zero Trust approach

Develop a zero-trust infrastructure, and move to a "trust-but-verify" philosophy.

### Incident Response Plans

Develop Incident Response Plans, test those plans, and act on any lessons learned from those tests.

**References:**
DORA: Why it is relevant to you | PwC. https://www.pwc.com/hu/en/szolgaltatasok/risk-assurance/dora-why-it-is-relevant-to-you.html
Digital Operational Resilience Act (DORA) | EIOPA. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

JUNGLE IT

# Ready to speak to an expert?

Ensuring your company's first line of defence is informed, prepared, alert and ready. Our Security team aims to arm your people with the knowledge and tools to keep your business safe.

If you're ready to improve your organisation's cyber security approach, or have any questions, we're here to help.

**Request a discovery call**

hello@jungleit.co.uk
0113 258 4433

jungleit.co.uk