DORA, which stands for the Digital Operational Resilience Act, comes into effect in 2025, however the guidelines for it are still apparently being written.

DORA, is a European Union (EU) regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector.

Although applicable to the financial sector, it's heavily focused on the supply chain in this sector, especially from a cyber resilience perspective, and therefore applies to any organisation that interacts with the financial sector in the third party chain. Although it's an EU directive, UK companies are going to be affected by this.

DORA provides a regulatory framework on digital operational resilience under which all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. It ensures that every organization has got the right security and data protection protocols in place and are operating those.

The responsibility for the governance of DORA is with the Board of directors but all departments, employees, contractors, vendors and partner agencies must observe and abide by all "Acceptable Use policies and procedures" pertaining to any owned ICT assets.

Although it is an EU directive, are companies or organizations in other jurisdictions affected and liable? Yes, any organisation which is part of the critical supply chain to banks trading in Europe would find it very hard to state that it only trades in the UK, especially if it has European outlets or components.

Fundamentally, DORA will ensure that any cyber due diligence undertaken by organisations during contract negotiations, investment, merger and acquisition, will be more indepth. Any financial entity is going to have to prove that they've done the right level of due diligence on their supply chain.

Keys areas for governance involve developing a Risk Framework and developing ICT Solutions for Data Protection and Business Continuity. There must be Resilience Testing for the strategies. In addition, there must a methodology for reporting ICT-Related Incidents and managing Third-Party Risk. plus effectively pen testing to help manage the incidents. Evidence of testing and the type of penetration testing should be stated in the contract requirements between any parties.

Evidence is the key here – as with so much surrounding Data Privacy and IT risk Management. Organisations must also ensure they have a forum for Information and Intelligence Sharing

DORA Checklist

- Develop a digital operational resilience strategy with KPIs and risk metrics
- Create a communication strategy for ICT incident disclosure
- Formulate a plan for resilience testing
- Establish an ICT risk framework
- Define roles and responsibilities for ICT risk management
- Develop policies and procedures for managing ICT risks and incidents. -.
- Implement independent assurance mechanisms to assess framework effectiveness.
- Implement ICT solutions for data protection and business continuity

- Conduct regular resilience testing, including threat-led penetration testing
- Assess ICT controls' effectiveness and identify vulnerabilities
- Establish a process to report incidents to authorities within 72 hours
- Manage risk from critical ICT service providers through due diligence and monitoring
- Participate in information sharing platforms to exchange best practices and threat indicators
- Implement a robust cybersecurity framework.
- Upgrade to the latest security software and hardware
- Train employees on cybersecurity best practices1
- Have a plan for responding to incidents