SOLUTION BRIEF

Unpacking DORA: Ensuring Digital Operational Resilience

As technology continues to permeate every aspect of our lives, with the financial sector as a frontrunner, we now have successfully digitized nearly every aspect of a bank. With the increased digitization of financial services comes increased dependency on digitized services. Everyone, therefore, needs these digitized systems to be resilient in order to serve the needs of people and businesses optimally around the globe. That's why the European Union introduced the Digital Operational Resilience Act (DORA) which will come into force in 2025 – so it's time to prepare.

What is DORA?

The Digital Operational Resilience Act (DORA) framework is designed to enhance the operational resilience of the EU's financial sector by establishing a comprehensive set of requirements for entities that provide financial services within the European Union. The act includes requirements for risk management, incident reporting, digital operational resilience testing, and third-party risk management. DORA's primary objectives are to:

- Establish a uniform set of standards for financial institutions to ensure the safe and secure provision of digital services.
- Improve the ability of financial institutions to prevent, quickly and adequately detect, and respond to cyber threats.
- Streamline and harmonize existing regulations to provide a single, cohesive regulatory framework.

Why do financial services companies need to ensure compliance with DORA?

Compliance with DORA is critical for several reasons:

- **Regulatory Requirements:** Financial institutions operating in the EU are legally required to adhere to DORA regulations. Non-compliance can result in regulatory action, including fines and penalties.
- **Enhanced Operational Resilience:** Compliance with DORA ensures that financial institutions have the necessary processes and controls in place to mitigate the risk of digital disruptions, which helps maintain the stability of the financial system.
- **Customer Trust:** Demonstrating a commitment to digital operational resilience by complying with DORA builds trust with customers, who increasingly demand secure and reliable digital services from their financial institutions.
- **Competitive Advantage:** Compliance with DORA can provide a competitive advantage by showcasing a commitment to cybersecurity and operational resilience, which can help attract and retain customers.

What are the consequences of non-compliance and lack of resilience?

Failure to comply with DORA regulations can have several adverse consequences for financial institutions on an operational and financial level, but also in terms of brand loyalty. Not only do they risk regulatory penalties, reputational damage and loss of business, but they also run an increased risk of operational disruption.

Why financial institutions should turn to Tanium to achieve DORA compliancy.

Tanium is the industry's only provider of converged endpoint management (XEM). Applying XEM dramatically improves the management of complex security and technology environments. Only Tanium protects every team, endpoint, and cloud from cyber threats by integrating IT, Compliance, Cybersecurity, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. This makes Tanium uniquely positioned to assist financial services organizations within the EU to become compliant.

Tanium helps in several ways:

Centralized management

Typically, banks have multiple environments (think workstations, mainframe, cloud, IAAS, legacy environments) that are being managed by different service providers. Typically, all these environments are managed with a diverse set of networking and security tools. Make no mistake, DORA rules apply to all these different environments and put the responsibility for hygiene and resilience back to the actual owner of these environments - the banks themselves. These different environments usually do not communicate and collaborate well with each other, so breaches and suspicious lateral movement may not be detected in time, and it is difficult to get a complete overview of all the assets the company is held responsible for. This is where Tanium comes in and solves exactly that with its Converged Endpoint Management (XEM) platform: from a central location, the entire endpoint infrastructure can be managed and controlled. That helps streamline hygiene efforts and reduces the time and materials required to achieve compliance.

Real-time visibility

Tanium's platform provides organizations with real-time visibility into all their digital assets, thus allowing them to identify and assess risks and remediate across their digital infrastructure, any place, any time, and in seconds - not hours, days or weeks.

Real-time prioritization

Risk prioritization can help IT teams evaluate the IT infrastructure beyond data vulnerabilities to help determine which vulnerabilities to patch and to assess an endpoint's security level – which can dramatically change the risk level. By prioritizing risks, security teams can more effectively allocate their already limited resources to focus on mission-critical tasks.

Real-time and automated compliance checks

Tanium ensures real-time and automated compliance checks by continuously monitoring endpoints on their data, users, configurations, and software (Bill of Materials). It employs advanced algorithms to compare this data against predefined compliance policies, generating alerts and remedial actions when violations are detected, thus enabling swift and proactive compliance management.

Real-time risk mitigation/remediation

Leveraging its comprehensive endpoint visibility and control platform, Tanium swiftly identifies vulnerabilities, assesses risks, and initiates immediate response actions across all endpoints. This proactive approach ensures rapid threat detection, containment, and remediation, thus minimizing potential damage and enhancing one's overall security posture.

Real-time incident response

Tanium continuously monitors and collects data from endpoints, thus providing instant visibility into security incidents. With its rapid query and response capabilities, Tanium enables organizations to quickly investigate and remediate threats, thus minimizing the impact of security incidents.

End-to-end or full-cycle processes for compliance management in a single platform

Tanium streamlines compliance management with its integrated platform. Through a sequential process (discover, assess, prioritize, mitigate, automate, validate, and evaluate) Tanium enables end-to-end handling of compliance processes. This comprehensive approach ensures efficient management and oversight, all within a single platform.

Why work with Tanium?

Financial services companies need to collaborate with Tanium for compliance with DORA because of the huge amount of work that needs to be done to comply. IT departments need to be able to easily automate and scale their activities and processes and Tanium is the only technology that can do that reliably and resiliently across all assets with a single platform. Tanium provides instant visibility into their IT infrastructure, empowering real-time monitoring, and threat detection. Its extensive control capabilities allow efficient management of assets, configurations, and vulnerabilities.

Tanium's unparalleled speed enables rapid response to security incidents and compliance requirements. Its platform technology and multiple integrations with well-established vendors facilitate streamlined process operations. By partnering with Tanium, financial services companies gain a comprehensive solution that addresses their compliance needs with efficiency, agility, and enhanced security.

Tanium works closely with a portfolio of partners who can assist organizations in advising on DORA and implementing the solutions required.