SOLUTIONS_

Simplifying DORA Compliance with Eclypsium

The Digital Operational Resiliency Act (DORA) is the landmark cybersecurity regulation for the EU's financial sector, mandating requirements for managing ICT risks and third-party relationships. As of January 2025, organizations will need to have the tools and processes in place to maintain and document their compliance. Eclypsium arms teams with unique capabilities to meet these requirements by automatically identifying and mitigating risks at the hardware and firmware level and verifying the integrity of ICT assets.

DORA EXTENDS TO HARDWARE, FIRMWARE, AND THE SUPPLY CHAIN_

DORA extends to any areas that can pose risk to the availability or integrity of the service or customer data. And like most modern security standards, this includes physical assets in the enterprise (and their firmware), and likewise, a firm's technology supply chain. This can be seen in how DORA defines the following terms.

> **ICT Asset** - ... any "*software or hardware asset in the network and information systems used by the financial entity.*"
>
> **ICT Services** - "*... digital and data services provided through ICT systems... including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider...*"
>
> **ICT Risk** - "*... any reasonably identifiable circumstance... that may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment ...*"

These broad definitions effectively state that if an ICT issue can cause risk, then it is in scope. The regulation heavily focuses on any assets that if compromised, would impact the availability of service or the integrity of data. This means security must include end-user computing devices such as laptops and desktops, servers and other data and application infrastructure, and even networking infrastructure. And all of these concerns likewise extend to third-party service providers. Simply hiring a third party or buying an asset does not absolve the firm from its security requirements. Organizations must evaluate prospective service providers in terms of security and actively hold them accountable.

ADDRESSING DORA REQUIREMENTS WITH ECLYPSIUM_

While regulatory compliance goes well beyond the capabilities of any one security tool, there are several key areas where Eclypsium addresses DORA requirements that otherwise might be missed.

1. Risk Management

DORA Requirements	How Eclypsium Helps
Article 6 requires organizations to "protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers" and that these requirements extend to "computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures."	Eclypsium provides simple automated scans down to the lowest levels of software, firmware, and physical components within an asset. Likewise, the solution can be applied to a wide range of asset types including laptops as well as servers and networking infrastructure that often can't support a traditional security agent.

2. Asset Inventory

DORA Requirements	How Eclypsium Helps
Article 8 further requires teams to "identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment." Teams must then establish and maintain inventories of those assets and hardware.	Eclypsium can create and audit a detailed inventory of assets including granular insight into all critical firmware and physical components within an asset.

3. Change Management

DORA Requirements	How Eclypsium Helps
Article 9 also requires organizations to "implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters...to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner."	Eclypsium proactively identifies any out-of-date firmware, firmware vulnerabilities, or low-level misconfigurations or missing protections. The system can then help prioritize updates based on real-world threat intelligence and assist staff with applying necessary device-level updates.

NEXT STEPS_

These are only some of the ways that Eclypsium can help address DORA's many requirements. For example, Eclypsium offers unique capabilities in the areas of threat detection (Article 10) and incident response (Article 11) by exposing both known and unknown backdoors and implants, which attackers often use to maintain persistence and evade traditional EDR tools. Furthermore, DORA requires firms to proactively assess their third-party service providers and perform regular audits to ensure they adhere to security standards. Eclypsium scans can ensure that teams have real, technical visibility during these audits instead of simply taking a vendor's word.

To learn more about the Eclypsium solution and how it applies to DORA as well as other regulatory standards such as NIS2, please reach out to the Eclypsium team at info@eclypsium.com.