





Meet DORA Requirements with LayerX





The Digital Operational Resilience Act (DORA) is an EU regulation that strengthens the financial sector's resilience against ICT risks and cyber threats. It provides a unified framework to ensure financial entities can endure, respond to, and recover from digital disruptions, enhancing the stability of the EU financial system amidst growing digitalization and cyber challenges.

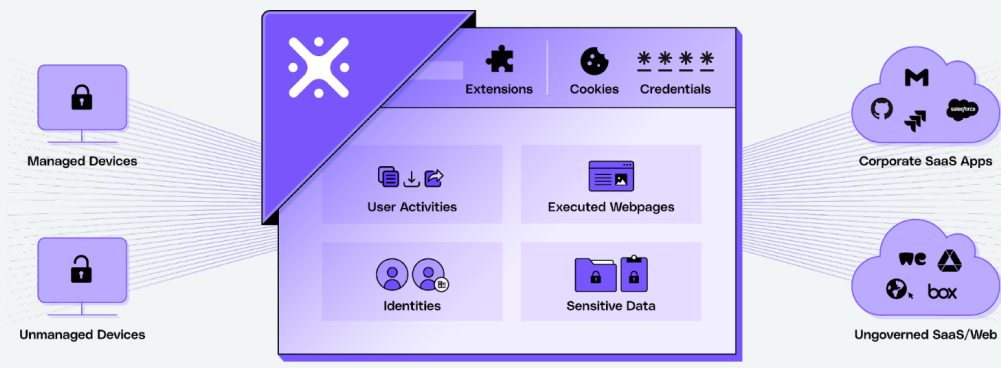
DORA entered into effect on 16 January 2023 and will apply from 17 January 2025. This time frame provides financial entities with a two-year implementation period to comply with its requirements.

For financial institutions governed by DORA, LayerX provides visibility, control, and risk management capabilities for all browser-based user activity and data, helping organizations meet DORA requirements and enhance their security posture.

Below is a more detailed explanation on how LayerX can help organizations address each of the requirements of DORA:

DORA Requirement		How LayerX Can Help You
	<p>ICT Risk Management</p> <p>Financial entities are required to implement robust ICT risk management frameworks that can identify, assess, and mitigate ICT-related risks.</p> <p>This includes mapping ICT systems and dependencies between systems and processes, conducting continuous risk assessments, classifying cyber threats, and analyzing the business impact of risks.</p> <p>Institutions are also required to add protection measures, like identity and access management policies, patch management, and security controls.</p>	<p>The browser is the nerve center of the modern workplace. This means financial organizations adhering to DORA are required to include the browser in their ICT risk management plans.</p> <p>LayerX provides full visibility and control over identities, accounts, applications, data, and user activity in the browser workspace.</p> <p>This includes:</p> <p>Mapping & risk assessment:</p> <ul style="list-style-type: none"> • Detecting, tracking, and cross-correlating all browser identities, accounts, profiles, websites/applications, browsers, devices, and extensions. • Tracking all user activity in the browser, including browsing, text input, copy/paste, file upload/download, printing, cookie usage, and more. • Detection, risk analysis and management of browser extensions. • Detection, risk analysis and management of Shadow SaaS. <p>Threat classification:</p> <ul style="list-style-type: none"> • Classifying GenAI application and website risks. • Classifying credential and password risk. <p>Protection measures:</p> <ul style="list-style-type: none"> • Enforcing identity rules and access management on SaaS apps. • Enforcing browser updates to ensure use of the latest version.
	<p>ICT 3rd-party Risk Management</p> <p>Risk management also applies to ICT third-party service providers. This includes contractual agreements, as well as security controls.</p>	<p>Most websites nowadays contain third-party code components, which can bring vulnerabilities or malware into the organizational network. LayerX provides a built-in AI-powered analysis engine, based on a neural network, which actively monitors every web page – and every individual object within each page – identifying third-party malicious elements and automatically blocking them. This enables comprehensive protection from web attacks and ensures secure browsing.</p>

DORA Requirement		How LayerX Can Help You
 <p>Oversight of Critical 3rd-party providers</p>	<p>The browser is a key channel for third-party access to organizational assets such as SaaS applications, information sharing, etc. LayerX can be used as an authentication method for secure least privilege access to the organization's SaaS and web applications, from managed and unmanaged devices, locations, and for any user (employees and 3rd party), replacing the need to use costly and complex VPN and VDI solutions.</p>	
 <p>Digital Operations Resilience Testing</p> <p>Financial institutions need to conduct regular testing of ICT systems, including advanced threat-led penetration testing for certain entities.</p>	<p>LayerX provides a full audit of all users, identities, accounts, SaaS applications, browsers and browser extensions, helping organizations to map-out their threat surface, identify weak spots, and direct resilience testing measures to those areas.</p>	
 <p>ICT-related incidents</p> <p>Entities must establish processes for monitoring and detecting ICT-related incidents, as well as reporting major incidents to competent authorities.</p>	<p>LayerX provides a centralized graphical management console for monitoring, logging, alerting and policy creation, and security management, where all browser-related threats can be monitored and used for reporting purposes.</p>	
 <p>Information sharing</p> <p>DORA encourages the exchange of cyber threat information and intelligence among financial entities to enhance collective resilience.</p>	<p>LayerX Labs is the research division of LayerX, focusing on identifying and analyzing emerging online cyber threats. These findings are published to our customers, and when necessary, we also create security policies to address these vulnerabilities. LayerX encourages customers to share Layer Labs' threat information further to enhance overall browser security and protect the financial industry from sophisticated cyber threats.</p>	



LayerX Enterprise Browser Extension natively integrates with any browser, turning it into the most secure and manageable workspace, with no impact on the user experience.

LayerX is the first solution that provides continuous monitoring, risk analysis, and real-time enforcement on any event and user activity in the browsing session.

Enterprises leverage these capabilities to secure their devices, identities, data, and SaaS apps from web-borne threats and browsing risks that endpoint and network solutions can't protect against. These include data leakage over the web, SaaS apps and GenAI tools, credential theft over phishing, account takeovers, discovery and disablement of malicious browser extensions, Shadow SaaS, and more.

[Learn more about LayerX enterprise browser solution.](https://layerxsecurity.com)