everbridge™

Harnessing DORA

Empowering financial services through resilience and innovation

How operationalizing DORA compliance through holistic security platforms can create strategic advantages now and in the future.

By Lorenzo Marchetti
Head of Global Public Affairs

In a fast-changing world where digital transformation drives competition, the financial services sector is under pressure to maintain business resilience, protect employees, and stay ahead through innovation. In this context, one of the main regulations from the European Union, Digital Operational Resilience Act (DORA), stands out more than just a compliance mandate; rather, it reconciles the operational resilience and compliance-driven innovation for institutions in the financial sector. Indeed, DORA compliance can be leveraged to enhance resilience and build a competitive edge.

Everbridge is here to help by providing customers with a complete solution that digitizes organizational resilience. Offering a suite of powerful tools to help know earlier, respond faster, and improve continuously.

If you'd like to learn more about industry solutions for DORA, visit our website at everbridge.com or request a demo.

Understanding DORA: How to ensure operational resilience

The DORA regulation is designed to secure the operational resilience of financial institutions (FIs) in the face of digital disruptions. Its core purpose is to protect the integrity of the financial system by enforcing robust risk management and ICT (information and communication technology) standards.

To do so, the fundamental requirement of DORA is to enable operational resilience. The comprehensive regulatory framework helps FIs to manage and mitigate ICT risks through clear guidelines and standards before, during, and after a disruptive incident. DORA mandates FIs to identify potential threats and vulnerabilities through regularly testing their ICT systems, including vulnerability scanning, penetration testing, and threat-based red teaming. Once an incident occurs and has an impact on the financial interests of clients, DORA mandates that FIs report significant ICT incidents to regulatory authorities, implement effective incident response within 24 hours, and submit a final report outlining further details of the incident and its resolution within 72 hours to prevent recurrence. It also requires FIs to have plans in place for ensuring business continuity and disaster recovery.

24

Hours to report significant ICT incidents to regulatory authorities once an incident occurs which will have an impact on the financial interests of clients.

72

Hours to submit a final report outlining further details of the incident and its resolution.

Why DORA?

DORA was introduced by the European Commission in response to the increasingly dire cybersecurity environment affecting business operations. The growing reliance on technology in financial services has led to heightened vulnerability to operational disruptions, cyberattacks, and other ICT risks. According to the IMF's Global Financial Stability Report, the number of cyberattacks has almost doubled since before the COVID-19 pandemic due to growing digital connectivity and rising geopolitical tensions.[1] Cyber incidents have cost the global financial sector an estimated $12 billion in direct losses over the past two decades. The exposure to cyber risks is significant: financial firms have been targeted in nearly one-fifth of all reported cyber incidents, with losses reaching $2.5 billion since 2020.

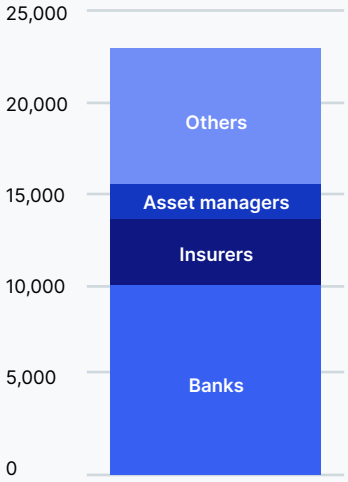
While the median direct loss reported by firms from cyber incidents has remained relatively modest at $0.4 million, the high level of interconnectedness among FIs significantly increases the risk of widespread impact. When cyber disruptions occur at one financial institution, they are likely to cascade to others, particularly as financial firms become increasingly reliant on common third-party IT providers.

A notable example of this risk is the 2016 cyberattack that targeted the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a secure messaging system used globally by over 11,000 FIs to process transactions. During the attack, cybercriminals infiltrated Bangladesh Bank's local systems and manipulated the SWIFT Alliance Access software to bypass security protocols. The attackers planted malware to conceal fraudulent transaction requests and sent 35 payment requests to the Federal Reserve Bank of New York totaling $951 million. Due to a spelling error in one of the transfer requests, most transactions were flagged, and only five were processed, resulting in the loss of $81 million to the Bangladesh Bank.[2] Though a more significant loss was avoided by the lapse of the attackers in that case, it could have been prevented through a more systemic approach.

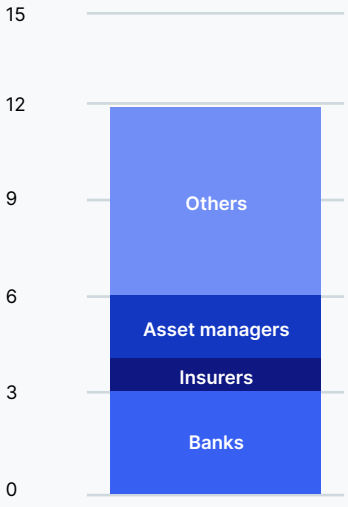
Attractive target

The financial sector has suffered more than 20,000 cyberattacks, causing $12 billion in losses, over the past 20 years.

Financial sector cyber incidents
(number, 2004-23)



Financial sector losses
(billions of US dollars, 2004-23)



Source: Advisen cyber loss data and IMF staff calculations.

[1] IMF, Global Financial Stability Report (International Monetary Fund, 2024), 77, Global Financial Stability Report.

[2] KPMG, Bangladesh Hack Illustrates Rising Sophistication of Attacks (2016), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/08/swift-it.pdf.

The management of ICT third parties is an integral component of the DORA framework to address increasing incidents of data breaches. According to the regulation, FIs must identify their third-party ICT dependencies and ensure that critical functions are not overly reliant on a single provider or a small group of providers.[3] They are also expected to actively manage ICT third-party risks. When outsourcing critical functions, financial firms need to establish clear contractual agreements that cover aspects such as exit strategies, audits, and performance targets for accessibility, integrity, and security, among other key considerations. Besides ICT third-party risk management, DORA also mandates that FIs have strong incident response, notification, and recovery plans that address both internal and external stakeholders during a crisis. According to Article 11 ("Response and recovery"), "financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures, and mechanisms." The comprehensive DORA framework is devised to help FIs mitigate the risks posed by evolving cyber disruptions and minimize downtime whenever an incident is identified. The precautions, incident management, and recovery mechanisms enable operational resilience for FIs throughout each stage of an IT outrage.

Besides ICT third-party risk management, DORA also mandates that financial institutions have strong incident response, notification, and recovery plans.

[3] Anna Eugenia Omarini, "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future," International Business Research 11, no. 9 (2018): 23-37, https://www.ccsenet.org/journal/index.php/ibr/article/view/76769.

Innovation through compliance: The path to operationalize DORA

DORA as a regulation does not stifle innovation in the financial sector by imposing overly stringent restrictions. Instead, innovation can emerge from operationalizing the compliance with such regulations, as demonstrated by similar cases in the financial sector. BBVA, a leader in the financial services industry, was one of the first banks to leverage another regulatory change -- the EU's Payment Services Directive 2 (PSD2) -- as an opportunity to innovate and drive customer-centric solutions. Compliance with PSD2 required BBVA to open its financial data to third-party service providers, which could have been seen as a challenge to its market position. However, BBVA transformed this regulatory mandate into a strategic initiative for innovation by launching an open banking platform to third parties via the BBVA APIMarket. This open platform allowed fintechs and startups to access BBVA's core services and develop new financial services. BBVA created new revenue streams through partnerships. The compliance-driven push toward opening their infrastructure enabled BBVA to monetize its API platform while maintaining customer trust and security.[3]

Similarly, HSBC's investment in AI technology was initially driven by the need to comply with anti-money laundering (AML) regulations and enhance operational resilience. In December 2021, HSBC was fined £63.9 million by the UK's financial regulator, Financial Conduct Authority, on the grounds of "unacceptable failings" of its anti-money laundering systems. These failings involved inadequate scenario coverage, deficient parameter settings, and data integrity issues. HSBC's transaction monitoring systems did not sufficiently cover the necessary risk indicators for detecting money laundering and terrorist financing. It also failed to ensure the completeness and accuracy of data fed into its monitoring systems, which resulted in the incorrect or incomplete monitoring of millions of transactions.[4]

[3] Anna Eugenia Omarini, "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future," International Business Research 11, no. 9 (2018): 23-37, https://www.ccsenet.org/journal/index.php/ibr/article/view/76769.

[4] Financial Conduct Authority, Decision Notice: HSBC Bank PLC, December 14, 2021, https://www.fca.org.uk/publication/decision-notices/hsbc-bank-plc.pdf.

In response to these regulatory pressures, HSBC embraced innovation as a solution. To address these systemic deficiencies and build greater operational resilience, the bank partnered with Google Cloud to develop an AI-powered solution capable of identifying suspicious activities with higher precision. The AI tools originally designed for compliance were later adapted to offer[5] improved credit risk assessment services, personalized loan offerings, and fraud prevention measures. This strategic shift not only enabled HSBC to rectify its compliance shortcomings but also led to broader technological advances. HSBC's deployment of AML AI was so successful that it earned the Celent Model Risk Manager of the Year 2023 award.

Similarly, DORA presents significant opportunities for innovation. To achieve its goal of enhancing digital resilience, DORA needs to be not only adopted, but operationalized. Financial institutions will need to invest in holistic security platforms, both digital and physical, that ensure their processes are integrated and uninterrupted. These platforms empower institutions to proactively manage risks, enhance service offerings, and develop new revenue streams. This approach not only aligns with regulatory demands but also drives the development of cutting-edge solutions that can redefine the competitive landscape.

By positioning themselves at the forefront of technological advancement, financial institutions can transform regulatory compliance into a strategic advantage. The journey towards operational resilience under DORA is not merely a regulatory obligation but a pathway to pioneering leadership in an evolving digital landscape. Through advanced solutions like those offered by Everbridge, financial entities can transform regulatory mandates into opportunities for growth and innovation. This partnership not only ensures regulatory compliance but also enhances the institution's resilience and adaptability in an ever-evolving digital world, positioning them to thrive in a complex and competitive regulatory landscape.

The journey towards operational resilience under DORA is not merely a regulatory obligation but a pathway to pioneering leadership in an evolving digital landscape.

[5] Richard D. May, "Fighting Money Launderers with Artificial Intelligence at HSBC," Google Cloud Blog, September 30, 2023, https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence.

About Everbridge

Everbridge empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

Visit Everbridge.com

Read our company blog

Follow us on LinkedIn

Follow us on X

Get in touch to learn about Everbridge, empowering resilience.

WP-EN-HarnessingDORA:EmpoweringFinancialServices_10.28.24