



SafeBreach

WHITE PAPER

Enhancing Digital Operational Resilience with SafeBreach in the DORA Era

Learn why enterprise security leaders are choosing the SafeBreach exposure validation platform to help them navigate Digital Operational Resilience Act (DORA) compliance with confidence.

Contents

| | |
|--|-----------|
| Executive Summary | 3 |
| DORA: Driving a New Era of Resilience | 4 |
| Background & Establishment | |
| Implications for Financial Institutions | |
| DORA's Global Reach: Why Non-EU Institutions Should Still Pay Attention | |
| SafeBreach's Exposure Validation Platform: Powering Proactive Cyber Defense | 6 |
| SafeBreach Validate: Continuous Security Control Testing at Scale | |
| SafeBreach Propagate: Visualizing Post-Breach Blast Radius | |
| How SafeBreach Maps to DORA Requirements: A Practical Alignment Guide for Compliance & Resilience Teams | 7 |
| Future-Proofing for the EU Cyber Resilience Act & Beyond | 9 |
| Why SafeBreach? | 9 |
| Conclusion | 10 |
| Appendix | 11 |

Executive Summary

Financial institutions are facing a perfect storm: a rapidly evolving threat landscape and the growing complexity of digital infrastructure. Against this backdrop, financial institutions across the European Union (EU) specifically are entering a new era of cybersecurity accountability. The Digital Operational Resilience Act (DORA)—which went into effect in January 2025—marks a significant regulatory shift, mandating that these organizations move beyond reactive audits and toward continuous assurance of their digital defenses.

For the first time, institutions must demonstrate—on an ongoing basis—that their cybersecurity controls are effective, resilient, and aligned with evolving threats. DORA introduces binding requirements for real-time risk management, resilience testing, third-party oversight, and harmonized standards across all EU member states. These mandates demand a fundamental transformation in how financial entities validate, monitor, and report on their security postures. Traditional security assessments—like point-in-time audits and manual penetration tests—are no longer sufficient. What's needed is continuous, automated, and intelligence-driven validation of defenses.

SafeBreach, the leader in enterprise security validation, enables institutions to meet DORA's most critical requirements through its **exposure validation platform**. By simulating real-world threats across the MITRE ATT&CK® framework, SafeBreach helps organizations continuously test control effectiveness, uncover hidden risks, and validate detection and response capabilities. Crucially, the SafeBreach platform goes beyond simple detection, providing actionable remediation guidance that helps teams prioritize and resolve vulnerabilities based on real-world risk and business impact.

This whitepaper will provide a high-level overview of DORA regulations, including the forces behind its creation and its implications for financial enterprises. It will also outline how SafeBreach—through its core solutions **Validate** and **Propagate**—helps financial institutions operationalize DORA compliance through ongoing threat emulation and prioritized remediation insights. Finally, it will provide a direct mapping of SafeBreach capabilities to key DORA articles, providing a practical framework for implementation.

DORA: Driving a New Era of Resilience

Background & Establishment

DORA is a landmark regulation introduced by the EU to strengthen the IT security and operational resilience of financial institutions across member states. It was formally adopted by the European Parliament and Council in December 2022, and entered into force on January 16, 2023. Following a two-year implementation period, DORA became fully applicable across the EU on January 17, 2025.

Regulatory Drivers

The creation of DORA was driven by several converging forces:

- Increased frequency and sophistication of cyberattacks targeting the financial sector, including ransomware, supply chain attacks, and cross-border threats.
- Fragmented cybersecurity regulations across EU member states, leading to inconsistent resilience standards and regulatory gaps.
- Heavy reliance on third-party Information and Communication Technology (ICT) service providers, including cloud, infrastructure, and software vendors whose security practices were often outside the direct control of financial entities.
- Digital transformation across financial services, which accelerated during the COVID-19 pandemic and exposed operational dependencies and resilience blind spots.

To address these challenges, DORA was proposed as part of the EU Digital Finance Package in September 2020, alongside other initiatives aimed at boosting digital innovation and financial stability. The regulation represents the first EU-wide framework specifically focused on digital operational resilience in the financial sector.

Purpose: A Catalyst for Change

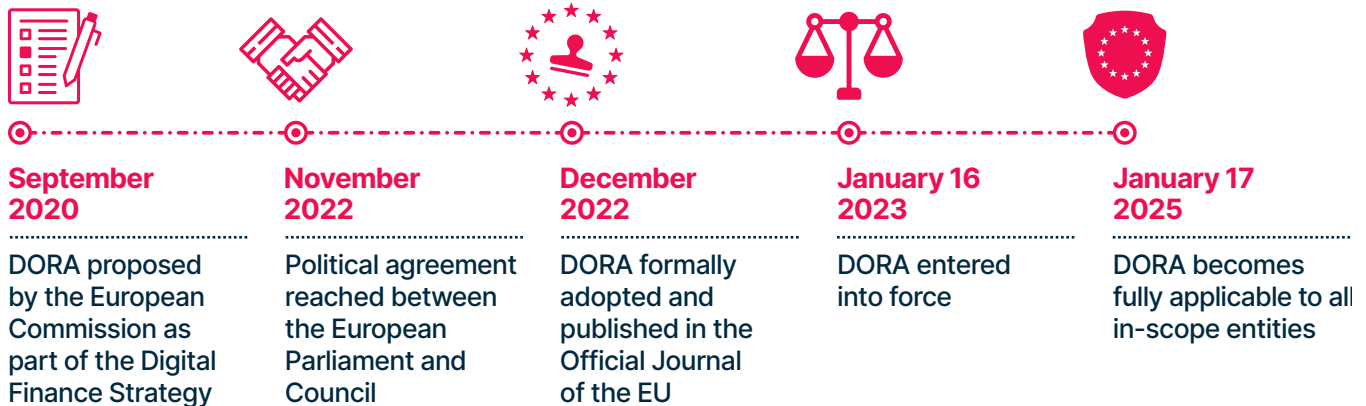
DORA applies to a broad spectrum of financial entities—including banks, insurers, investment firms, crypto-asset service providers, and critical ICT third-party providers—across all EU member states. Its cross-sectoral scope and binding nature mark a significant regulatory advancement, establishing a unified digital resilience baseline for the European financial ecosystem.

Crucially, DORA recognizes that traditional, periodic compliance checks are no longer sufficient in today's dynamic threat landscape. It mandates real-time visibility into cyber risk, continuous validation of control effectiveness, and proactive preparedness for increasingly sophisticated attacks—particularly those stemming from complex third-party and supply chain dependencies.

HIGH-LEVEL GOALS OF DORA

- **Enhanced Cyber Resilience.** Rigorous, continuous testing of ICT systems to ensure readiness against modern threats.
- **Harmonization Across the EU.** A unified standard for cyber resilience to ensure consistency and cross-border trust.
- **Proactive Risk Management.** Continuous validation of cybersecurity controls, with real-time remediation insights.
- **Operational Continuity & Trust.** Confidence that financial services will remain operational during and after cyber incidents.

Key Milestones in DORA's Legislative Journey



Implications for Financial Institutions

As noted above, DORA compels financial institutions to adopt a proactive cybersecurity posture, with specific requirements around ICT risk management, incident reporting, resilience testing, and third-party risk oversight. The regulation raises the bar for compliance expectations—and introduces substantial penalties for non-compliance.

DORA stipulates fines that can reach up to 2% of an entity's total annual worldwide turnover or up to 1% of the company's average daily worldwide turnover for ongoing breaches.

Turnover, in this context, refers to gross revenue—the total income generated before any expenses are deducted. It includes all global earnings, not just EU or financial-sector revenue. This penalty model, similar to that used by the General Data Protection Regulation (GDPR), ensures fines are proportionate to a company's overall scale and economic footprint.

Additionally, individuals like senior executives, may face personal fines of up to €1 million for compliance failures—underscoring the importance of leadership accountability in resilience planning and execution.

DORA's Global Reach: Why Non-EU Institutions Should Still Pay Attention

While DORA is a regulation enacted by the EU, its impact is not limited to organizations headquartered within EU borders. Financial institutions and ICT service providers operating globally still fall under DORA's scope if they serve EU-based clients or operate branches, subsidiaries, or critical infrastructure within EU member states.

Some key considerations for non-EU institutions include:

IN-SCOPE ACTIVITIES, NOT JUST LOCATION

DORA applies to financial entities and critical third-party providers delivering services into the EU financial sector, regardless of their geographic origin. If your organization supports EU-based financial institutions—whether through cloud infrastructure, cybersecurity services, or data processing—you are obligated to comply with relevant provisions or potentially face severe penalties.

CONTRACTUAL & SUPERVISORY OVERSIGHT

Under DORA, financial institutions must ensure third-party providers—including those outside the EU—adhere to its resilience standards. This often translates into contractual requirements, due diligence, and supervisory coordination, which can affect your service agreements and operational responsibilities.

REPUTATIONAL & COMMERCIAL PRESSURE

Even when DORA does not apply directly, alignment with its principles can be a competitive differentiator. Demonstrating proactive cyber resilience, auditability, and continuous control validation can support trust, regulatory alignment, and partnership opportunities across the EU market.

Ultimately, DORA is setting a global precedent for operational resilience. Organizations outside the EU that want to remain relevant partners to the European financial ecosystem should consider adopting DORA-aligned practices—and platforms like SafeBreach provide a streamlined, scalable path to doing so.

SafeBreach's Exposure Validation Platform: Powering Proactive Cyber Defense

To comply with DORA requirements, financial institutions need more than visibility—they need empirical evidence that their defenses work as expected against today's dynamic and sophisticated cyber threats. The SafeBreach exposure validation platform delivers exactly that, combining breach and attack simulation with attack path validation to give organizations an end-to-end, real-time view of their true security posture.

SafeBreach Validate: Continuous Security Control Testing at Scale

SafeBreach Validate is an award-winning breach and attack simulation (BAS) solution designed to put your cyber defenses to the test—safely, continuously, and at enterprise scale. Using more than 30,000 attack methods from SafeBreach's industry-leading Hacker's Playbook™, Validate simulates adversarial behaviors across the MITRE ATT&CK® kill chain to:

- Continuously test the efficacy of security controls across endpoints, networks, cloud environments, and applications.
- Accelerate remediation by providing contextual insights and clear next-step guidance to resolve vulnerabilities and misconfigurations—tailored to the organization's environment and mapped to real-world threats.
- Provide security teams with step-by-step recommendations that streamline triage, reduce mean time to remediate (MTTR), and support DORA's emphasis on timely corrective action.
- Validate detection engineering by automating multi-stage attack scenarios and verifying alerting and response workflows.
- Support regulatory reporting and audit readiness through empirical data and structured dashboards.
- Measure and monitor cyber risk using customizable reporting aligned with business outcomes and threat frameworks.

Validate does not execute actual malware. Instead, it simulates phases of real-world attacks in a safe and controlled manner, ensuring enterprise-grade safety and zero impact on production systems.

SafeBreach Propagate: Visualizing Post-Breach Blast Radius

SafeBreach Propagate extends validation beyond perimeter defenses by simulating attacker movement within the network—providing visibility into how an adversary could exploit internal pathways to reach critical assets. Designed with an “assumed breach” mindset, Propagate complements Validate by simulating lateral movement and post-compromise scenarios like ransomware propagation and credential theft.

Propagate’s key capabilities include:

- Mapping high-risk attack paths to organizational crown jewels.
- Evaluating post-breach exposure through credential harvesting, subnet scanning, and lateral movement simulations.
- Prioritizing remediation based on business impact and proximity to sensitive assets.
- Enhancing communication through structured, stakeholder-ready dashboards and reports.
- Ensuring enterprise safety and compliance, with customizable testing scopes, encrypted credential handling, and impact-limiting controls.

With Propagate, security teams can accurately assess the blast radius of a successful breach and make data-driven decisions to fortify internal defenses.

How SafeBreach Maps to DORA Requirements: A Practical Alignment Guide for Compliance & Resilience Teams

As financial institutions navigate the evolving landscape of the Digital Operational Resilience Act (DORA), translating regulatory intent into operational action is critical. This section provides a practical guide to understanding how SafeBreach aligns with DORA—both at a strategic level and at the level of specific regulatory articles.

The first table presents a high-level view, linking SafeBreach’s core capabilities to the operational and compliance benefits they enable. The second table offers a more granular mapping, aligning these capabilities directly to relevant DORA articles to help organizations assess coverage, demonstrate alignment, and identify potential gaps.

Together, these resources are designed to support security and compliance leaders in operationalizing resilience and achieving measurable, audit-ready outcomes under DORA.

SafeBreach Capabilities & Benefits



Continuous Security Validation

30,000+ threat simulations across MITRE ATT&CK

Ongoing detection of misconfigurations and control gaps

Alerts on failed detections to accelerate remediation



Regulatory Reporting & Audit Support

Audit-ready reports detailing test outcomes, gaps, and resolutions

Custom dashboards for board-level visibility

Supports continuous tuning of detection logic



Third-Party & Supply Chain Risk

Tests resilience against compromised third-party tools or services

Identifies potential propagation paths via supplier networks

Supports integrated risk management strategies



Incident Detection & Response

Tests SOC alert fidelity and response timelines

Measures detection capabilities of SIEMs and EDR tools

Supports continuous tuning of detection logic

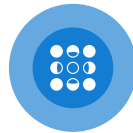


Threat-Led Penetration Testing

Emulates lateral movement, privilege escalation, and post-breach activities

Validates defenses against real-world threat actors

Helps meet requirements for advanced adversarial simulation



Scenario-Based Testing & Cyber Drills

Simulates complex, multi-stage attacks, including ransomware, data exfiltration, and insider threats

Enables red team–blue team exercises and tabletop drills

Supports regulatory-mandated cyber exercises



Risk Management & Cyber Resilience

Automated, environment-wide testing (endpoints, networks, cloud, applications)

Visual mapping of attack paths to crown jewels

Prioritized remediation with prescriptive guidance based on risk exposure, asset sensitivity, and exploitability—supporting DORA's requirements for effective incident prevention and risk mitigation

Mapping DORA Requirements to SafeBreach Capabilities

| DORA Requirement | DORA Article | SafeBreach Capability |
|--|---------------------------|--|
| Continuous testing of ICT systems | Article 5, Article 10 | Validate + Propagate with 30,000+ real-world simulations |
| Incident response and recovery testing | Article 10(2), Article 11 | Scenario-based simulations, SOC validation |
| Audit-ready reporting | Article 12, Article 15(5) | Structured reports and dashboards |
| Third-party and supply chain risk | Article 28, Article 30 | Simulations covering third-party integrations |
| Threat-led penetration testing | Article 26, Article 27 | Advanced post-breach and lateral movement testing |

Future-Proofing for the EU Cyber Resilience Act & Beyond

While DORA focuses on the financial sector, the upcoming EU Cyber Resilience Act (CRA) will broaden the scope to include all digital products and services. SafeBreach's continuous validation approach positions organizations to meet CRA's future requirements around software resilience and secure-by-design practices. SafeBreach also ensures that resilience is not a one-time checkbox, but a living, evolving capability. Its platform supports adaptive strategies to meet future regulations and evolving attacker tactics.

Why SafeBreach?

ACTIONABLE REMEDIATION, NOT JUST TESTING

SafeBreach goes beyond simply simulating attacks—it delivers clear, prioritized remediation guidance so teams know exactly what to fix and where to start. This ensures faster resolution, enhanced audit readiness, and stronger alignment with frameworks like DORA.

UNIFIED EXPOSURE VALIDATION STRATEGY

When deployed together, SafeBreach Validate and SafeBreach Propagate offer a full-spectrum view of your cybersecurity posture—before and after a breach. This integration transforms breach and attack simulation (BAS) into a proactive, continuous engine for operational resilience, compliance assurance, and strategic risk reduction.

PROVEN AT SCALE

Backed by the industry's most comprehensive attack simulation engine, SafeBreach includes over 30,000 threat methods across real-world attack chains—ensuring relevance and depth at enterprise scale.

PRODUCTION-SAFE BY DESIGN

SafeBreach never uses actual malware, ensuring zero impact on live systems. This makes it safe to run continuously in complex, regulated production environments.

FAST TIME-TO-VALUE

With prebuilt templates and intuitive dashboards, SafeBreach accelerates compliance alignment and makes it easier for security teams to demonstrate value early.

BUILT FOR COMPLEX ENVIRONMENTS

Especially tuned for the financial sector, SafeBreach supports intricate infrastructures with granular control scopes that map to organizational realities.

INTEGRATED, IMPACTFUL REPORTING

Empirical results are tied directly to business and regulatory outcomes, making it easier for security leaders to communicate value and readiness to executives and auditors.

WORLD-CLASS SUPPORT

Backed by world-renowned threat researchers and an award-winning customer success team that provide a level of service and support not available anywhere else.

Conclusion

DORA—and the impending CRA regulations—represent a fundamental shift in how institutions must approach cyber resilience—moving from periodic assessments to a model of continuous oversight and proactive defense. SafeBreach enables organizations to meet these evolving mandates through its comprehensive exposure validation platform. By combining the power of SafeBreach Validate and SafeBreach Propagate, institutions gain the ability to continuously test their defenses, understand the true impact of potential breaches, and prioritize remediation based on business risk. Together, these tools support a forward-leaning strategy for regulatory compliance, operational continuity, and long-term cyber resilience.

DORA is not just another regulation—it's an opportunity to build a stronger, more resilient cybersecurity foundation. SafeBreach is ready to help your organization meet the moment.

Connect with us today to learn how SafeBreach can future-proof your digital operational resilience strategy.

Appendix

Glossary

| | |
|-------------------------|--|
| BAS | Breach and Attack Simulation |
| CRA | Cyber Resilience Act |
| DORA | Digital Operational Resilience Act |
| EDR | Endpoint Detection and Response |
| ICT | Information and Communication Technology |
| MITRE ATT&CK | A globally-accessible knowledge base of adversary tactics and techniques |
| MTTD | Mean Time to Detect |
| SIEM | Security Information and Event Management |
| SOAR | Security Orchestration, Automation, and Response |
| SOC | Security Operations Center |

About SafeBreach

SafeBreach is the leader in enterprise-grade exposure validation, providing the world's largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach Exposure Validation Platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit SafeBreach.com.



All content ©SafeBreach 2025.
All rights reserved.

