Scapien

White Paper

Bringing Order to Chaos
Simplifying DORA Compliance for Financial Services with Scapien

Bringing Order to Chaos: intelligent Security Risk Management

Author: Atul Chowdhry
Date: January 10, 2026

Table of Contents

Executive Summary

The Digital Operational Resilience Act (DORA) is fundamentally reshaping the cybersecurity landscape for financial services firms across the EU. For small and medium-sized enterprises (SMEs), navigating these stringent requirements is both critical and challenging. In a market saturated with multipoint solutions yielding mediocre results—and where cybersecurity spending fatigue is prevalent—organisations need a comprehensive yet manageable approach to security and regulatory alignment.

Scapien's intelligent Security Risk Management (SRM) solution, iPAS™, is designed to meet the needs of SMEs. Aligned with Gartner's SRM framework, iPAS integrates critical functions—including penetration testing, remediation management, and broader security validation—into a unified platform. This consolidation delivers measurable security improvements while reducing operational overhead, helping SMEs strengthen resilience and support DORA compliance without inflating budgets or overburdening their teams.

The Problem: Challenges of DORA Compliance for SMEs

Regulatory Pressure

The Digital Operational Resilience Act mandates rigorous Information and Communications Technology (ICT) requirements for EU financial services firms to strengthen cybersecurity and operational resilience. One component is Threat-Led Penetration Testing (TLPT), which requires in-scope organisations to conduct realistic assessments of their exposure to cyber threats. These assessments must prioritise identified security risks based on business impact and maintain auditable records of remediation efforts.

For entities classified as significant, TLPT involves threat-led scenarios tailored to the organisation's risk profile, with independent testing performed on a supervisory cycle typically set at around three years, unless the competent authority specifies otherwise. DORA encourages the use of recognised methodologies—such as TIBER-EU—when designing and executing these exercises.

Compliance with DORA is not optional for in-scope EU financial entities. Non-compliance can lead to severe penalties, operational disruptions, and reputational damage—consequences that can be particularly devastating for SMEs.

Operational Challenges for SME Financial Services Firms

Financial services SMEs face significant hurdles in meeting DORA's stringent requirements. Resource constraints are a primary challenge, as smaller organisations often operate with limited budgets and minimal cybersecurity expertise. This makes it difficult to conduct the advanced assessments required under DORA's TLPT and ICT risk management expectations, which demand specialised skills and continuous monitoring capabilities.

Risk visibility presents another critical challenge. The difficulty of connecting technical vulnerabilities to business operations often hinders meaningful prioritisation. An SME may identify a security flaw in its payment processing system or customer data storage environment, but translating that into business level risk—financial fraud exposure, regulatory penalties, or loss of customer trust—remains a major obstacle. This gap makes it harder for management to allocate resources effectively to the issues that truly matter.

DORA's Technical Requirements and Testing Mandates

DORA establishes explicit and prescriptive expectations for how EU financial institutions must structure and operate their ICT risk management frameworks. At its core, the regulation requires firms to maintain ongoing security testing and validation to ensure that their controls remain effective against evolving threats. This includes a combination of vulnerability assessments, targeted security evaluations, and penetration testing conducted at a frequency proportionate to the organisation's risk exposure.

For entities designated as significant by their supervisory authority, DORA introduces Advanced Threat-Led Penetration Testing (ATLP). These exercises must emulate realistic threat scenarios relevant to the institution's operations, carried out by independent, qualified testers and informed by recognised methodologies. Frameworks such as TIBER-EU may be used as references when designing and executing these engagements, helping institutions model adversary tactics in a controlled and safe manner. ATLP is generally performed on a multi-year supervisory cycle, with the specific frequency determined by the competent authority.

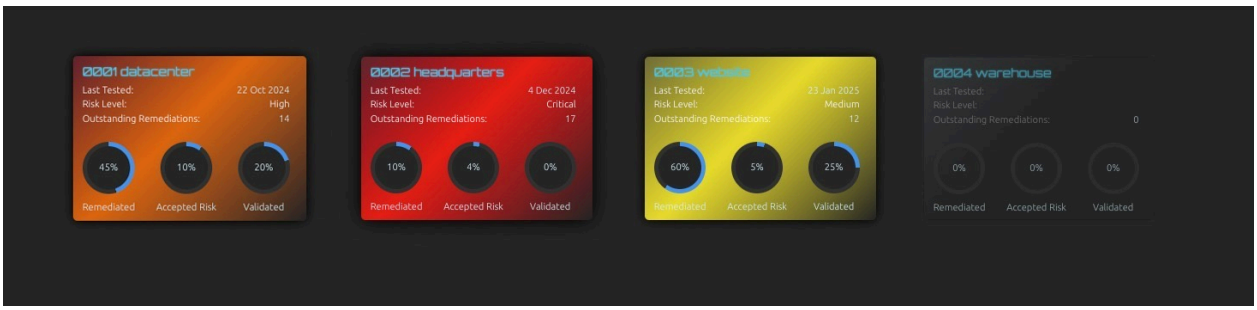
DORA's ICT risk management obligations extend well beyond testing. Financial institutions must maintain detailed inventories of all business functions, processes, roles, and information assets within their ICT landscape. They are required to assess the risks associated with critical third-party providers on a recurring basis, reflecting DORA's heightened emphasis on supply-chain resilience. Institutions must also document and test their incident response and business continuity plans, ensuring they include defined recovery objectives and clear communication procedures for security incidents.

Documentation and auditability are central elements of DORA. Institutions must maintain evidence of testing activities, control validations, remediation progress, and governance decisions. Regular reporting to senior management and supervisory authorities is mandatory, and firms must be able to demonstrate a consistent methodology for assessing ICT risk and validating the effectiveness of controls over time.

How Scapien Addresses These Challenges

Scapien addresses DORA's testing and control-validation requirements through a hybrid methodology powered by the intelligent SRM platform iPAS™. The platform begins by identifying security risks using attacker-logic security, combining adversarial simulation with automated network discovery to reveal how real-world threats might move through internal, external, and cloud environments.

iPAS then progresses into deeper threat identification and validation through knowledge-driven automated testing modeled on real threat actors and penetration testers. Its outputs emphasise zero-noise findings that have been validated for accuracy, enabling teams to focus on security issues with genuine operational or regulatory impact rather than raw alerts.



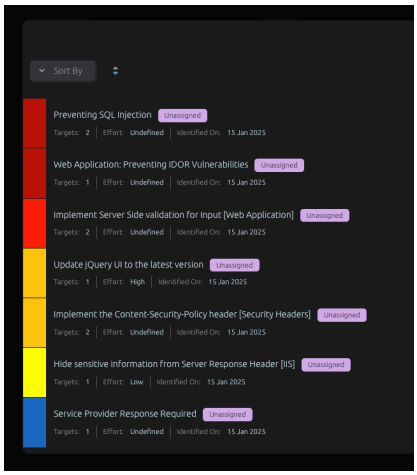
Throughout this process, iPAS maintains continuous validation across the entire environment, helping financial institutions demonstrate ongoing control effectiveness in line with DORA's expectations. Scapien's analysts review and confirm findings to ensure fidelity and relevance, combining automation with expert oversight to produce reliable, actionable results.

Additionally, iPAS's security risk identification, prioritisation, and tracking capabilities bridge the gap between technical findings and business impact. By mapping validated security risks to concrete operational and regulatory outcomes, iPAS helps organisations understand which weaknesses matter most and why. This context-aware approach ensures that remediation efforts focus on the most critical risks, supporting effective resource allocation and strengthening overall resilience.

Implementation Methodology and Operational Integration

Scapien's implementation approach prioritises immediate security value while establishing a foundation for long-term operational resilience. The process begins with a comprehensive environment analysis that sets baseline security metrics and identifies critical assets requiring protection. This initial assessment phase anchors continuous improvement efforts and supports early alignment with DORA's ICT risk management expectations.

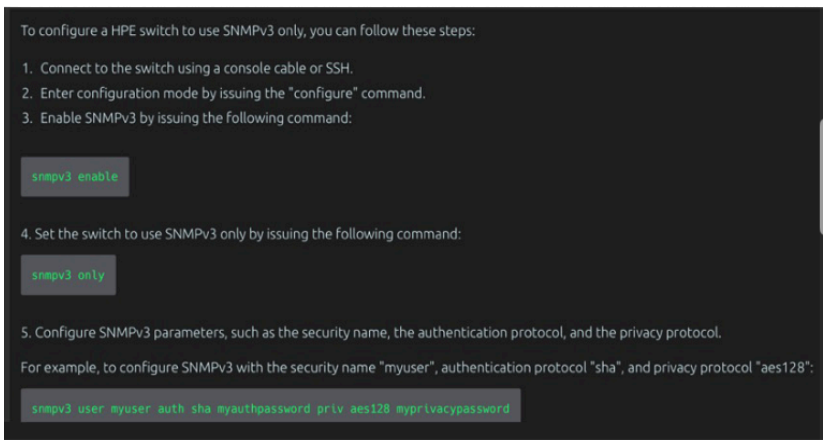
The solution is deployed within carefully controlled parameters to ensure production safety, even in sensitive financial environments. This addresses a key concern for financial institutions: the need to conduct meaningful security testing without risking operational disruption. Scapien's ability to operate safely within live environments enables ongoing control validation and security assessment without compromising system stability.



Operational Benefits and Risk Reduction

The operational impact of implementing Scapien's platform extends well beyond meeting DORA's minimum requirements. Institutions gain enhanced visibility into their security posture through real-time risk tracking and ongoing control validation. This enables the automatic establishment of a continuous security awareness programme, supporting proactive management rather than periodic, reactive assessments. With iPAS, organisations can run frequent evaluations, monitor remediation progress, and ensure vulnerabilities remain resolved once validated. This prevents previously remediated risks from re-emerging and strengthens long-term resilience against malicious activity.

In the critical area of remediation management, Scapien provides detailed, step-by-step technical guidance for addressing identified security risks. This includes explicit remediation actions and follow-up validation testing to confirm the effectiveness of implemented controls. For financial institutions with limited internal security expertise, this structured guidance is especially valuable, enabling teams to remediate efficiently, maintain a stronger security posture, and optimise resource allocation.



Audit and Compliance Documentation

The platform maintains comprehensive audit trails for every security risk identified, aligning with DORA's documentation and evidence requirements. Each finding, remediation action, and validation test is automatically logged and preserved, creating an unbroken chain of evidence that supports supervisory review. This automated record-keeping significantly reduces the administrative burden typically associated with compliance while ensuring completeness and accuracy of documentation.

Security and compliance reporting are also streamlined through the platform. iPAS generates detailed reports suitable for internal stakeholders and regulatory authorities, clearly demonstrating ongoing testing activities, remediation progress, and overall control effectiveness. Its ability to maintain historical testing and remediation records is particularly valuable during audits, providing clear, defensible evidence of the organisation's security posture and sustained commitment to regulatory compliance.

Future Security Capabilities

As cyber threats continue to evolve, Scapien's platform development focuses on increasing the depth, coverage, and automation of security testing. Upcoming capabilities include enhanced asset discovery and classification features, enabling more precise risk assessment and prioritisation across complex environments. The platform's expanding artificial intelligence capabilities will strengthen its knowledge base, threat detection, and risk forecasting while preserving the essential balance between automated efficiency and expert validation.

Competitive Differentiation

In today's cybersecurity landscape, financial services organisations often face a choice between traditional penetration testing firms and automated security tools. Traditional firms provide point-in-time assessments that, while thorough, leave significant gaps between evaluations. These periodic engagements do not meet DORA's expectation for ongoing control validation and often produce lengthy reports highlighting theoretical vulnerabilities rather than actionable insights.

Automated security tools, although capable of continuous scanning, frequently generate high volumes of false positives and lack the contextual understanding required for business-context risk prioritisation. Because these tools focus primarily on technical findings without linking them to operational or regulatory impact, organisations struggle to allocate resources effectively and risk creating compliance gaps.

Scapien's hybrid approach resolves these limitations by combining human + machine teaming with attacker-logic security to deliver deeper and more reliable assessments. The platform's knowledge-driven testing methodology maintains broad and detailed coverage while providing zero-noise output—validated, accurate findings mapped directly to business risks. This approach ensures that institutions focus their efforts on the issues that matter most, supported by high-fidelity intelligence that strengthens operational resilience and supports DORA-aligned security governance.

Total Cost of Ownership and Resource Optimization

Financial institutions implementing Scapien's platform typically see substantial gains in the efficiency of their security operations. The reduction in false positives, combined with clear and structured remediation workflows, enables security teams to focus on genuine risks rather than theoretical vulnerabilities. With zero-noise output and findings mapped to business-context risk prioritisation, teams spend far less time sifting through irrelevant alerts and more time addressing issues that materially affect security and compliance.

The platform's integrated compliance reporting capabilities further reduce operational overhead by automating the documentation required under DORA. This automation extends beyond generating reports, supporting continuous tracking of security improvements and validation testing over time. It provides complete and defensible evidence of compliance efforts without adding administrative burden, enabling organisations to demonstrate their operational resilience with confidence.

Conclusion

As DORA compliance becomes mandatory for financial services organisations, the demand for efficient and effective security solutions is increasingly critical. Scapien's iPAS platform meets this need by delivering comprehensive security testing, actionable remediation guidance, and automated compliance documentation. Its ability to provide validated, high-fidelity security insights—supported by zero-noise output and reduced operational overhead—makes it especially valuable for SMEs operating with limited resources.

By combining continuous validation, practical remediation guidance, and automated compliance reporting, Scapien enables organisations to meet DORA's expectations while strengthening their overall security posture. Its emphasis on business-context risk prioritisation ensures that security teams focus on issues that genuinely matter for operational resilience and regulatory alignment. As cyber threats evolve and regulatory demands expand, Scapien's ongoing platform enhancements ensure that financial institutions can maintain compliance and security effectiveness without overburdening their teams.

Call to Action

Financial services organisations seeking to meet DORA's compliance requirements while strengthening their security posture should consider how Scapien's iPAS platform aligns with their operational and regulatory needs. By delivering comprehensive security testing, practical remediation guidance, and automated compliance reporting, the platform enables institutions to achieve and maintain compliance while optimising limited resources.

We invite you to schedule a consultation with our security experts to explore how Scapien can support your DORA compliance efforts. This discussion will focus on your specific regulatory obligations and demonstrate how the platform can address your organisation's security and operational challenges.

Contact us now to learn more: Email: contactsales@scapien.com Telephone: +1 (307) 314-4182