ECB Guide Targets Harmonized Cyber Testing Approach

By **Simon Onyons and Nebu Varghese** (March 26, 2025)

Simon Onyons

Nebu Varghese

The financial sector faces a constantly evolving landscape of cyber threats, further amplified by the rapid advancement of technologies like artificial intelligence.

In response to this evolution, on Feb. 11, the European Central Bank issued updated guidance to the threat intelligence-based ethical red teaming, or TIBER-EU, threat-led penetration testing framework, further looking to harmonize operational resilience testing practices across the European Union.[1]

TIBER-EU is a framework that tests an organization's resilience against sophisticated attacks by simulating real-world cyber threats that leverage threat intelligence[2].

This is a significant step forward. The evolution of sophisticated technologies can introduce vulnerabilities and expand an organization's attack surface. These changes demand a proactive and adaptive approach to cybersecurity.

While traditional methods like ethical hacking and penetration testing remain valuable, they are no longer sufficient on their own to address the complexities of today's threat landscape. This is particularly crucial moving forward, as organizations increasingly rely on AI-enabled technologies, which require specialized testing methodologies to identify and mitigate potential vulnerabilities.[3]

Threat-led penetration testing, which emphasizes threat intelligence and realistic attack simulations, has emerged as a critical tool for ensuring the resilience of financial institutions against evolving threats.

In response to this dynamic environment, financial services regulators across the globe have intensified their focus on cybersecurity, introducing new legislation and refining existing frameworks to bolster the operational resilience of financial institutions, including the recent update to TIBER-EU. This update is material, aligning TIBER-EU with the Digital Operational Resilience Act, or DORA, and its requirements for threat-led penetration testing.[4]

This article explores implications for financial sector institutions. It analyzes key changes introduced by the updated TIBER-EU framework, provides practical guidance on navigating the complexities of DORA compliance, and highlights the importance of a unified approach to cybersecurity testing in the face of evolving threats.

Rise of Threat-Led Penetration Testing

DORA, which came fully into effect on Jan. 17, introduces a comprehensive set of rules for the digital operational resilience of the financial sector.[5] A key component of DORA is the mandate for systemically important institutions, or those with mature information and communication technology systems and processes, to conduct threat-led penetration

testing.[6]

Threat-led penetration testing is a sophisticated approach to cybersecurity assessments that simulates real-world cyberattacks to identify vulnerabilities and improve defenses. Threat-led penetration testing goes beyond traditional penetration testing by incorporating threat intelligence specific to the organization and its operating environment. This facilitates a more targeted and realistic assessment of an organization's ability to withstand sophisticated cyberattacks, moving beyond simply identifying technical vulnerabilities, to understanding how an organization's people, processes and technologies would respond under pressure.[7]

By simulating the tactics, techniques and procedures of real-world threat actors, threat-led penetration testing provides a more accurate picture of an organization's cyber resilience and demonstrates how the organization's immune response will function under realistic conditions, with appropriate risk management controls in place.

This intelligence-driven approach is critical in keeping pace with today's dynamic threat landscape, where cyber-attacks are becoming increasingly sophisticated and targeted, often exploiting vulnerabilities in human behavior and organizational processes, in addition to technical weaknesses.

TIBER-EU 2.0

The updated TIBER-EU framework provides a standardized methodology, with clearly established timelines, for conducting threat-led penetration testing. This aligns with DORA's requirements and promotes a harmonized approach across the EU, enabling financial institutions to benchmark their practices against a common standard and fostering collaboration across borders where similar regimes are in place.

Key changes introduced include the following.

Stricter Timelines

DORA introduces strict deadlines for deliverables in the threat-led penetration testing process, promoting efficiency and clearer expectations around compliance requirements. Meeting these deadlines is crucial to avoid potential regulatory penalties, emphasizing the need for organizations to proactively manage resources and engage red team service providers who can deliver within these constraints.

Mandatory Purple Teaming

Recognizing the value of collaboration, TIBER-EU now mandates purple teaming. Within cybersecurity, red, blue and purple teams represent distinct yet interconnected functions. The red team simulates malicious actors, proactively identifying vulnerabilities through controlled cyberattacks.

Conversely, the blue team acts as the organization's defense, monitoring systems and responding to security incidents. Purple teaming integrates these two functions, fostering collaboration between the red and blue teams. This approach cultivates a continuous feedback loop, collectively strengthening the organization's security posture by facilitating the sharing of attack techniques and defense strategies. This ultimately enhances the organization's security posture through a deeper understanding of both offensive and defensive cybersecurity practices.

Harmonized Terminology

The update aligns terminology with DORA standards, enhancing consistency with cross-border threat-led penetration testing regulations in other jurisdictions, such as Critical National Infrastructure Banking Supervision and Evaluation Testing in the U.K., and the Innovation Centre for Applied Sustainable Technologies in Hong Kong.

This includes replacing the term "white team" with "control team," ensuring clarity and consistency in communication between financial institutions and regulatory authorities. This harmonization of language facilitates smoother collaboration and compliance processes, not just within the EU, but also in a broader international context.

As a result, the updated TIBER framework promotes a more unified approach to operational resilience, ensuring that all stakeholders, regardless of their location or regulatory framework, are on the same page when it comes to threat-led penetration testing. This reduces the potential for confusion and misinterpretation, fostering greater cooperation and efficiency in cybersecurity efforts across borders.

Prescriptive Guidance and Provider Selection

The updated framework provides detailed guidelines for conducting threat-led penetration testing in a secure and structured manner, building on lessons learned from previous TIBER-EU tests. This ensures that testing is conducted to a high standard, minimizing risks and maximizing value.

The guidance covers all aspects of threat-led penetration testing, from scoping and threat intelligence gathering to testing execution and reporting. The new and improved guidance on assessing the quality of service providers, will allow financial service institutions to evaluate providers based on their experience, expertise and capabilities, and select partners who can deliver high-quality testing services.

This emphasis on provider selection underscores the importance of engaging with experts who possess a deep understanding of the TIBER-EU framework, DORA requirements, and the broader financial services threat landscape.

Simplified National Implementation

The implementation process has been streamlined to facilitate the adoption of the framework by EU national authorities, reducing complexity and promoting consistency across the EU. This ensures a more harmonized approach to threat-led penetration testing across the bloc, facilitating a cohesive and unified cybersecurity regulatory landscape.

Practical Implications for Financial Institutions

The TIBER-EU update has significant practical implications for financial institutions subject to DORA. Organizations must take the following steps.

Conduct a Gap Analysis

Financial institutions must conduct a comprehensive gap analysis to assess their current resilience testing practices against the updated TIBER-EU framework to identify areas for improvement. This analysis should encompass technical controls, governance, policies and human factors.

Select Qualified Experts

Selecting a provider to assist with threat-led penetration testing engagements requires careful consideration. Prioritize experience, expertise and a deep understanding of the regulatory landscape, together with collaborating with experts who have actively contributed to industry best practices and regulatory frameworks, and who maintain strong relationships with key national cyber agencies.

For organizations with a global presence, it is essential to consider providers with a robust international network and an in-depth knowledge of local regulatory nuances in the threat-led penetration testing space.

This approach is critical not only for successfully navigating the intricate web of cross-border regulatory compliance, but also for seamlessly facilitating collaborative testing efforts between different authorities.

It fosters an environment of mutual recognition and trust, assuring regulators in various jurisdictions that the rigorous standards of their respective frameworks have been upheld.

Internal Preparation

Adequate internal preparation is essential for effective threat-led penetration testing matters. This includes allocating resources, training staff and establishing clear communication channels. This internal preparation ensures that the organization is ready to actively participate in the threat-led penetration testing process, facilitating a smooth and productive engagement.

Importance of Unified Approach and Practical Takeaways

The TIBER-EU update underscores the importance of a unified approach to cybersecurity in the financial sector. By harmonizing threat-led penetration testing methodologies and aligning them with DORA requirements, the framework promotes consistency, efficiency and collaboration across the EU. This allows institutions to learn from each other's experiences, share best practices, and collectively strengthen their defenses against cyber threats.

This unified approach not only facilitates compliance, but also strengthens the overall cyber resilience of the financial sector. By working together and sharing knowledge, institutions can better protect themselves and their customers from evolving threats.

To effectively navigate this advancing landscape, financial institutions and legal professionals should consider the following practical takeaways.

Identify Applicable Regulatory Requirements

In an increasingly interconnected world, regulatory compliance is paramount. For financial institutions operating across borders, this means navigating a complex web of cybersecurity regulations, each with its own nuances and requirements.

Thoroughly identify and understand the cybersecurity regulations applicable to operations in each region, including those related to threat-led penetration testing. This includes mapping processes to those requirements to determine what additional considerations need to be made to annual regulator-mandated threat-led penetration testing processes.

Adopt Integrated End-End Test Approach

While not an explicit requirement of the TIBER-EU framework, organizations should consider leveraging integrated testing approaches, such as combining red teaming with tabletop exercises and adopting zero-warning approaches to testing frameworks, to maximize the value of the exercise, realize significant resource savings, and ensure a comprehensive assessment of their cyber resilience leveraging several interconnected testing approaches.

This comprehensive strategy provides a more nuanced understanding of an organization's cyber resilience, evaluating not only technical controls and incident response capabilities, but also the critical interplay between different teams, including executive management, during a simulated cyber-attack.

This approach can remove scenario challenge and exercise bias, and allows for a deeper understanding of both technical vulnerabilities and the nontechnical aspects of incident response, such as decision-making, communication and coordination between teams.

Value of Purple Teaming

Harness the power of collaboration through purple teaming. By bringing together red and blue teams, organizations can foster a more proactive and dynamic security posture, improving threat detection and response, accelerating remediation efforts, and cultivating a security-conscious culture.

This collaborative approach transcends traditional adversarial testing, creating a dynamic learning environment where both attack and defense perspectives are valued and leveraged to strengthen the organization's overall security posture.

Purple teaming offers numerous benefits, enhancing an organization's overall cyber resilience. By fostering collaboration between red and blue teams, it facilitates a more proactive security environment, improving the entity's ability to identify, analyze and respond to emerging threats. The collaborative identification and addressing of vulnerabilities enable swifter and more effective remediation, reducing the window of exposure.

Moreover, purple teaming cultivates a security-conscious culture across the organization, promoting knowledge sharing and raising awareness of cybersecurity risks and best practices.

By understanding the specific nuances of TIBER-EU and DORA, legal professionals can provide valuable guidance to their clients, ensuring compliance and contributing to a more secure and resilient financial sector. This expertise is crucial in navigating the complexities of the evolving cybersecurity landscape, enabling institutions to confidently face future challenges.

Simon Onyons is a managing director and Nebu Varghese is a senior director at FTI Consulting Inc.

affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html; https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf?0309990e5e167a47ca4748370a949064.

[2] https://www.ecb.europa.eu/.

[3] https://www.law.com/legaltechnews/2023/12/21/fortifying-the-future-the-crucial-role-of-red-teaming-as-ai-assumes-centre-stage/.

[4] https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc27919c71c17d5a10851_Financial%20Entities%20Ethical%20Red%20Teaming%20Framework.pdf.

[5] https://www.dora-info.eu/rts-tlpt/.

[6] https://www.dora-info.eu/rts-tlpt/.

[7] https://www.fticonsulting.com/insights/fti-journal/managing-risk-understanding-your-firms-obligations-under-dora.