Threat-Led Penetration Testing (TLPT) Policy

1. Introduction

At FundApps, we fully support the principles and objectives of the Digital Operational Resilience Act (***DORA***), particularly its emphasis on strengthening operational resilience and mitigating risks through robust Threat-Led Penetration Testing (***TLPT***). Our approach to TLPT reflects a commitment to fostering security and compliance within the financial sector and among all parties subject to DORA's requirements.

While we are committed to adhering to the rigorous standards set forth by DORA, our ethos extends beyond compliance to encompass the broader ecosystem of clients and services we support. We recognise that the implementation of TLPT must be approached with careful consideration to balance operational security, regulatory adherence, and the risk of unintended consequences.

Specifically, we aim to:

Minimise Collateral Impact: We acknowledge that TLPT activities, if not meticulously scoped and executed, may inadvertently impact other client environments that are not subject to DORA. These clients rely on our services for their operational stability, and we are steadfast in our commitment to minimising any risk of disruption to their critical operations.

Safeguard Client Regulatory Obligations: All of our clients operate within distinct regulatory frameworks and legal environments that impose specific filing requirements and disclosure obligations. It is essential that TLPT efforts do not inadvertently trigger obligations or breaches that could compromise their compliance posture.

This policy is designed to ensure that while we advance DORA-aligned objectives, we do so in a way that is collaborative, risk-aware, and protective of the unique needs and obligations of our diverse client base. By harmonising regulatory compliance with operational pragmatism, we aim to support the resilience of the financial ecosystem without compromising the integrity or obligations of any individual client.

2. Purpose

This policy establishes the framework for conducting TLPT for external testers and financial institutions (our clients) in compliance with the requirements set forth under the Regulatory Technical Standards (RTS) for TLPT as mandated by DORA. The objective of this policy is to ensure that ICT systems and services meet stringent operational resilience standards through rigorous, threat-informed testing methodologies.

This policy applies to:

- All external testers engaged by clients for TLPT engagements.
- Clients (including affiliates) utilising ICT services provided by FundApps to whom DORA applies.
- Internal personnel (for both Fundapps, clients and our respective affiliates) involved in coordinating or supporting TLPT activities.

3. Roles and Responsibilities

FundApps

- Facilitate collaboration between external testers and clients.
- Maintain oversight of TLPT activities, ensuring adherence to defined standards.

External Testers

- Conduct testing activities in strict accordance with the requirements of the RTS.
- Adhere to pre-approved testing scenarios, methodologies, and timelines.
- Provide detailed reporting of findings, including identified vulnerabilities and recommended remediation measures.
- External testers must demonstrate certifications, expertise, and independence to maintain the integrity of the testing process.

Clients (Financial Institutions)

- Assess the impact of the engagement and obtain sign-off from the relevant stakeholders.
- Provide necessary access and information to support TLPT activities.
- Facilitate collaboration between external testers and FundApps. This should include joint collaboration with FundApps on the preparation and scoping.
- Testing engagements must be supervised by qualified personnel to ensure compliance with RTS requirements and other applicable regulations.

4. Key Requirements

4.1. Frequency

One TLPT per client every three years, with a rotational schedule to balance demand. Testing must be limited to a test environment and not conducted in production or staging.

Testing must be scheduled during one of our two testing windows - January or November.

Requests must be submitted with at least 90 days' notice of intent to conduct TLPT. In the event that FundApps identifies multiple clients intending to conduct TLPT simultaneously, we will collaborate with all parties to coordinate a pooled TLPT.

4.2. Scope

To ensure consistency and scalability while adhering to DORA requirements, we ask clients to conduct testing within the parameters of a standardised scope for TLPT that applies to all clients. This ensures the tests focus on client-specific risks without overlapping into areas that affect shared SaaS infrastructure.

Included in Scope

Production-like User Interface

> Testers must refrain from testing live production environments. The client’s user interface contains sensitive and confidential information, including, but not limited to, data pertaining to client positions, disclosures, breaches, and other compliance-critical matters. Granting access to external testers entails inherent risks, including potential operational disruption and the compromise of a client’s compliance posture. The testing

will be on a separate, fully functional instance of the web application that simulates a live production environment. This approach ensures that testing activities can be conducted without compromising the confidentiality, integrity, or availability of the client's platform.

Dedicated APIs - limited to read-only APIs listed in our technical documentation.

Functional testing

- Includes authentication and authorisation, such as login flow
- Compromising a user account within the client's instance
- Attempting privilege escalation within the environment

Exclusions from Scope

The following areas are excluded:

- Making modifications to the system (i.e. any action such as making filings in a production system violates client agreements and constitutes a legal breach)
- Brute force attacks
- Any actions that would impact SLAs or uptime availability
- Shared infrastructure

4.3. Testing Methodology

Activities should minimise disruption to normal operations and adhere to agreed-upon timelines and objectives.

Pooled Testing

FundApps reserves the right to request pooled testing if it determines that TLPT should be permitted only when the quality or security of services provided to FundApps' clients—who are outside the scope of DORA—or the confidentiality of data related to such services, is reasonably expected to be adversely affected.

FundApps requires that a member of staff be appointed to the control panel for such pooled testing to enable FundApps to flag if any of the approaches suggested would impact the services or clients.

4.4. Protection of Data and Confidentiality

All data (if any) viewed, processed, obtained or generated during TLPT must be handled in compliance with;

- applicable data protection laws and standards, and
- FundApps Data Classification and Protection Standard.

Confidentiality agreements must be established with all parties involved in the TLPT process. Where FundApps is required to facilitate access to client confidential data in contravention of the terms of the agreement it has with a client, the client will need to provide explicit written consent in order for FundApps to accommodate this facilitation.

4.5. Reporting and Remediation

Findings must be documented in a detailed report, highlighting vulnerabilities, risks, and actionable remediation steps.

Reports must be shared with FundApps in a secure manner. Remediation timelines must be established and tracked, with progress reviewed periodically by both the client and FundApps.

4.6. Terms

Prior to commencement of any TLPT, FundApps, the client and external tester must enter into a tri-partite TLPT agreement.

5. Selection Criteria for External Testers

External testers must:

- Possess demonstrable experience in conducting TLPT for financial services.

- Have certifications such as CREST, OSCP, or equivalent.

- Operate with full independence and neutrality.

- Adhere to ethical standards and applicable legal frameworks.

- Have the requisite authority to view and have access to data (if any).

6. Incident Management

During TLPT, any detected security incidents must be immediately reported to the relevant FundApps contact.

Procedures for incident containment, mitigation, and reporting must align with and be handled in accordance with FundApps Incident Response Policy.

7. Recordkeeping and Documentation

All TLPT engagements must be documented, including scope, methodologies, findings, and remediation actions.

Records must be retained for the lifetime of the engagement with the client and a minimum of 7 years thereafter or as required by applicable regulations.

8. Policy Review and Updates

This policy will be reviewed annually or when significant regulatory or operational changes occur.

Updates will be communicated to all relevant stakeholders to ensure continued compliance and relevance.

9. Compliance

Non-compliance with this policy may result in the termination of contracts, suspension of FundApps participation in the TLPT or other legal consequences as appropriate.

10. Fees

Participating in TLPT within the standard scope will incur an hourly fee of £200 or as otherwise as agreed between the parties. This fee applies to all hours engaged in TLPT activities, including but not limited to related consultations.

Custom TLPT scenarios or testing outside the standard scope may incur additional costs and require separate agreements to be agreed between the parties