afine

digitally secure

TLPT DORA

Readiness Checklist

The Complete Operational Guide for Financial Entities

Book a TLPT consultation

Based on DORA RTS 2025/1190 | TIBER-EU 2025 Framework

Version 1.0 | March 2026

CONTENTS

How to Use This Checklist

Who this is for. Control team leads, CISOs, compliance heads, and anyone responsible for managing a TLPT exercise under DORA. Whether you are preparing for your first notification or refining your approach for a subsequent cycle, this checklist covers the full 12-18 month lifecycle.

How to work through it. The checklist follows the 8 phases of a TLPT in sequence. Work through each module as you progress. Check items off as you complete them. Some modules can overlap - see the timeline on the next page.

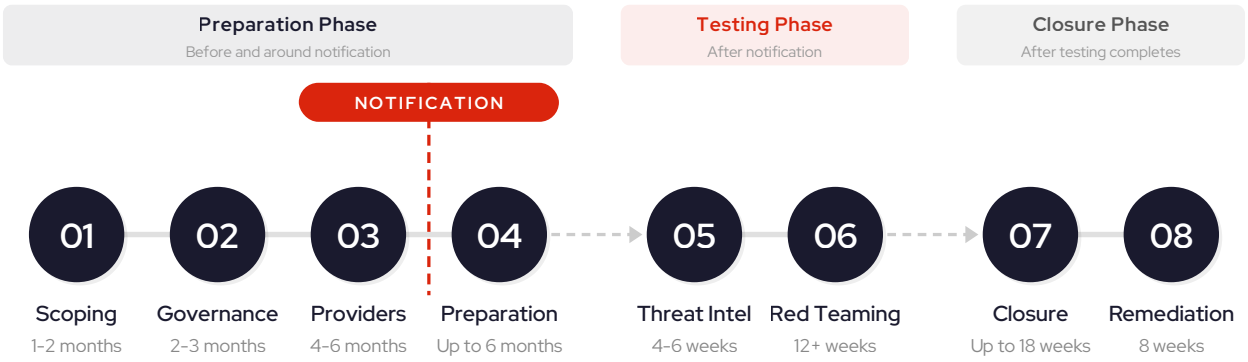
Every item has a regulatory reference. The monospace text after each item traces it to a specific article in the DORA RTS 2025/1190, DORA itself, or the TIBER-EU 2025 framework. Your legal and compliance teams can verify every requirement.

Priority levels indicate regulatory weight. CRITICAL items are regulatory requirements that block progress. HIGH items are strongly recommended. MEDIUM items are best practice.

Written by a red team. The practitioner tips throughout this document draw on years of offensive security and red team operations experience. They describe what goes wrong in practice and how to avoid it.

☐	Checkbox = action item to complete
CRITICAL	Regulatory requirement, non-negotiable
HIGH	Strongly recommended, failure causes delays
MEDIUM	Best practice, improves quality
RED TEAM INSIGHT	Practitioner tip from AFINE red team

TLPT Lifecycle Overview



Total duration: 18-28 months including pre-notification preparation. Post-notification minimum: 14-16 months.

Module Index

01 Am I In Scope?
DORA Art. 26 threshold and designation check

02 Governance Setup
Control team, secrecy protocols, CIF mapping

03 Provider Selection
TI and red team provider scoring and contracts

04 Preparation Phase
Project charter, scope spec, cross-border coordination

05 Threat Intelligence
Threat scenarios and TTI report for authority approval

06 Red Team Testing
12+ weeks active testing against live production

07 Closure Phase
Reporting, purple teaming, test summary

08 Remediation & Attestation
Remediation plan submission and formal sign-off

Key Deliverables at Each Gate

Annex I: Project Charter (3 months)

Annex II: Scope Specification (6 months)

Annex III: Targeted Threat Intelligence Report

Annex IV: Red Team Test Plan

Annex V: Red Team Test Report (T + 4 weeks)

Annex VI: Blue Team Test Report (T + 10 weeks)

Annex VII: Test Summary Report (A + 8 weeks)

Annex VIII: Attestation

Key Terms

Notification	Formal letter from your competent authority instructing you to conduct a TLPT. Day 0 - the regulatory clock starts here.
CTL	Control Team Lead - senior person managing the TLPT internally. Must have authority to act without disclosing details.
CIF	Critical or Important Function - business function that, if disrupted, would materially impair financial performance (DORA Art. 3(22)).
TI Provider	Threat Intelligence Provider - external firm that researches realistic attack scenarios for the TLPT.
TM	Test Manager - the TLPT authority's representative who oversees the test, approves scope changes, and validates results.
T, A	In deliverable deadlines: T = end of red team testing, A = attestation date.
BAU	Business As Usual - normal security operations, as opposed to TLPT-specific work.

01

Am I In Scope?

Determine whether your entity falls under the mandatory TLPT obligation based on DORA Article 26 thresholds, discretionary designation, or exemption eligibility.

Key deadline: Complete before formal notification

SCOPE

Module 01: Am I In Scope?

- [ ] Determine entity type - Are you one of the 21 types of financial entities under DORA Article 2?
  CRITICAL [DORA Art. 2(1)]

- [ ] Check mandatory thresholds (RTS Article 2): G-SII/O-SII credit institutions, payment institutions >EUR 150B, CSDs/CCPs automatically in scope, insurance >EUR 1.5B GWP
  CRITICAL [RTS Art. 2]

- [ ] Check discretionary inclusion - Even if below thresholds, your national competent authority may designate you based on impact, systemic character, ICT risk profile, or size
  HIGH [RTS Art. 2; DORA Art. 26(8)]

- [ ] Check exemption possibility - Competent authorities may exempt entities with low ICT risk profile even if technically in scope
  HIGH [DORA Art. 26(8)]

RED TEAM INSIGHT

Don't wait for formal notification. If you're close to the thresholds, start preparation now. The 3-month initiation deadline starts the day you're notified - and scoping without preparation work burns through that window fast.

RED TEAM INSIGHT

Entities regularly assume they're exempt because they fall below one threshold, only to get designated on discretionary grounds three months later. If your national authority has signaled interest in your ICT risk profile - or if peers in your sector have been designated - treat that as your starting gun.

02

Governance Setup

Establish the organizational infrastructure: management body buy-in, control team formation, secrecy protocols, and critical function mapping.

Key deadline: Start 6+ months before expected notification

TEAM

Module 02: Governance Setup

2A: Management Body Preparation

- [ ] Brief board/senior leadership on TLPT obligations and timeline (12-18 months)
  HIGH [DORA Art. 26(1); RTS Art. 9(6)]
- [ ] Confirm management body will be available to formally approve scope specification
  CRITICAL [RTS Art. 9(6)]
- [ ] Designate budget authority - typical TLPT costs EUR 150K-500K for TI + red team alone
  HIGH [Best Practice]
- [ ] Establish board-level reporting cadence for TLPT progress
  MEDIUM [RTS Art. 4; RTS Art. 9(4)]

2B: Control Team Formation

- [ ] Appoint Control Team Lead (CTL) with required authority and availability
  CRITICAL [RTS Art. 4; RTS Art. 9(4)]
  - [ ] Senior organizational standing with direct management access [RTS Art. 4]
  - [ ] Authority to make binding decisions without disclosure to other teams [RTS Art. 4]
  - [ ] Availability to dedicate significant time for 12-18 months [Best Practice]
  - [ ] Understanding of both business operations and ICT systems [RTS Art. 9(4)]
- [ ] Build control team (recommended 3-5 members)
  HIGH [RTS Art. 9(4)]
  - [ ] CTL (mandatory) [RTS Art. 4]
  - [ ] Risk/compliance representative [RTS Art. 9(4)]
  - [ ] ICT/infrastructure representative [RTS Art. 9(4)]
  - [ ] Business operations representative [RTS Art. 9(4)]
  - [ ] Legal/procurement representative (optional) [Best Practice]
- [ ] Establish secrecy protocols
  HIGH [RTS Art. 4]
  - [ ] Encrypted communication channels (separate from corporate email) [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Secure data room for TLPT documents [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Code name for the exercise [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Cover stories for control team meetings [RTS Art. 4]
  - [ ] Incident containment protocol if blue team detects red team activity [RTS Art. 4; RTS Art. 11(9)]

2C: Critical Function Mapping

- [ ] Identify ALL critical or important functions (CIFs) per DORA Article 3(22)
  CRITICAL [DORA Art. 3(22); DORA Art. 26(2)]

- [ ] For each CIF, map supporting ICT systems, outsourcing status, provider details, jurisdictions, and interconnections

  CRITICAL [RTS Art. 9(6); RTS Annex II]

  - [ ] Supporting ICT systems, processes, and technologies [RTS Annex II]
  - [ ] Outsourcing status (in-house vs. third-party provider) [RTS Annex II]
  - [ ] Provider name and contract reference (if outsourced) [RTS Annex II]
  - [ ] Jurisdictions where the function operates [RTS Annex II]
  - [ ] Interconnections with other functions/entities [RTS Art. 9(7)]

- [ ] Use the 7 criteria from RTS Article 9(7) to rank CIFs for inclusion

  CRITICAL [RTS Art. 9(7)]

- [ ] Prepare justification for any CIF excluded from TLPT scope

  CRITICAL [RTS Art. 9(6); RTS Annex II]

- [ ] Define preliminary flags for each in-scope CIF

  HIGH [RTS Annex II]

  - [ ] At least one targeting confidentiality [RTS Annex II; RTS Annex III]
  - [ ] At least one targeting integrity [RTS Annex II; RTS Annex III]
  - [ ] At least one targeting availability [RTS Annex II; RTS Annex III]

RED TEAM INSIGHT

The control team lead role is a full-time job disguised as a side responsibility. When the CTL is also running BAU security operations, scheduling problems surface by month three. If your CTL cannot block 60-70% of their calendar for the duration, appoint someone who can.

RED TEAM INSIGHT

Your cover story will be tested. When the blue team detects red team activity and escalates to incident response, the control team has roughly 30 minutes to contain the situation without blowing the exercise. Script your cover stories in advance and pressure-test them.

RED TEAM INSIGHT

Critical function mapping is the hardest part. Most banks don't have a clean mapping between business processes and ICT systems. Start this 6+ months before expected notification. Institutions regularly burn through their entire 6-month scoping window because they had to build this mapping from scratch.

03

Provider Selection

Evaluate, score, and contract threat intelligence and red team providers against RTS Article 7 minimum requirements and operational criteria.

Key deadline: Start 4-6 months before testing

VENDOR

Module 03: Provider Selection

3A: Threat Intelligence Provider - Minimum Requirements

- [ ] External to financial entity (mandatory - no internal TI for TLPT)
  CRITICAL [DORA Art. 27(2); RTS Art. 1]
- [ ] Manager with minimum 5 years threat intelligence experience
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Additional team member(s) with minimum 2 years experience
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Minimum 3 client references from previous TI assignments
  CRITICAL [TIBER-EU Procurement]
- [ ] Professional indemnity insurance covering misconduct and negligence
  CRITICAL [DORA Art. 27(1)(e); RTS Art. 7(1)]
- [ ] Certifications per recognized market standards
  HIGH [DORA Art. 27(1)(c); RTS Art. 7(1)]
- [ ] No conflict of interest with entity or involved ICT providers
  CRITICAL [RTS Art. 7(1)]
- [ ] Not simultaneously performing blue team tasks for the entity
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Separated from red team staff (if same company provides both)
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

3B: Red Team Provider - Minimum Requirements & Technical Competencies

- [ ] Test lead with minimum 5 years penetration testing and red team experience
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] At least 2 additional team members with minimum 2 years experience each
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Minimum team size: 3 persons with adequate replacement capacity
  CRITICAL [TIBER-EU Procurement]
- [ ] Minimum 5 client references from previous pentest/red team assignments
  CRITICAL [TIBER-EU Procurement]
- [ ] Professional indemnity insurance covering misconduct and negligence
  CRITICAL [DORA Art. 27(1)(e); RTS Art. 7(1)]
- [ ] Certifications per recognized market standards
  HIGH [DORA Art. 27(1)(c); RTS Art. 7(1)]
- [ ] No conflict of interest with entity or involved ICT providers
  CRITICAL [RTS Art. 7(1)]

- [ ] Not simultaneously performing blue team tasks for the entity
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

3B-TC: Technical Competency Assessment (16 areas)

- [ ] Open source intelligence gathering
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Exploit development
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Custom malware development
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Active Directory based exploitation
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Physical security testing
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] HID-based attacks
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] AV/EDR/NDR/XDR bypass
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Email security solutions bypass
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Secure web gateway bypass
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Anti-phishing solutions bypass
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Web/API/Mobile penetration testing
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Mainframe testing (if applicable)
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Wi-Fi penetration testing
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Social engineering
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Incident response knowledge
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Offensive security tool development
  MEDIUM [TIBER-EU Procurement 4.2]

3C: Contracting Essentials

- [ ] Define kill switch conditions and escalation path
  CRITICAL [RTS Art. 11(10); RTS Art. 5]
- [ ] Specify data handling: generation, storage, aggregation, reporting, destruction
  CRITICAL [DORA Art. 27(3); TIBER-EU Procurement]
- [ ] Define scope boundaries: what is permitted vs. prohibited
  CRITICAL [RTS Art. 11(1); RTS Annex IV]
- [ ] Include professional indemnity insurance requirements
  CRITICAL [DORA Art. 27(1)(e)]
- [ ] Specify weekly reporting cadence and format
  HIGH [RTS Art. 11(7)]
- [ ] Define leg-up process and approval chain
  HIGH [RTS Art. 11(8)]
- [ ] Address intellectual property and confidentiality
  HIGH [DORA Art. 27(3)]
- [ ] Include regulatory access provisions (TM may request reports)
  CRITICAL [RTS Art. 12(3)]
- [ ] If same company provides TI and RT: contractual separation of teams
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

RED TEAM INSIGHT

When evaluating red team providers, certifications tell part of the story. OSCE, OSED, OSEP, OSWE, and CRTO indicate the team can operate beyond standard penetration testing - custom exploit development, EDR bypass, full red team operations. CVE publications tell the rest: a provider that finds and responsibly discloses vulnerabilities in enterprise software (SAP, CyberArk, IBM, F5) demonstrates research depth that translates directly to TLPT quality.

RED TEAM INSIGHT

Provider rotation sounds simple until you try it. Your previous red team knows your environment, your detection gaps, and your incident response playbook. The new team starts from zero. Budget an extra 2-3 weeks in the TI phase for the new provider to get up to speed.

RED TEAM INSIGHT

Misalignment between the TI provider and the red team is one of the most common quality problems in TLPT engagements. The TTIR describes threat actors in abstract terms; the red team needs concrete attack paths. Demand a joint working session between TI and red team before the TTIR is finalized.

TI Provider Evaluation Criteria

#	Criterion	Weight	Score (1-5)
E1	Financial sector threat intelligence depth	High (3)	
E2	Target intelligence capability (HUMINT, OSINT, dark web)	High (3)	
E3	TLPT/TIBER prior experience	High (3)	
E4	Geopolitical and sectoral analysis capability	Medium (2)	
E5	Language capability for social engineering research	Medium (2)	
E6	Threat actor profiling methodology	High (3)	
E7	Scenario development quality	High (3)	
E8	Communication quality	Medium (2)	
E9	Data handling and destruction protocols	Medium (2)	
E10	Availability and responsiveness	Medium (2)	
E11	Report quality and actionability	High (3)	
E12	Team stability and replacement capacity	Medium (2)	
E13	Access to proprietary intelligence sources	Medium (2)	
E14	Collaboration track record with red teams	High (3)	
	WEIGHTED TOTAL (Max: 175)		

How to use. Rate each criterion from 1 (poor) to 5 (excellent). Multiply each score by the weight number in parentheses, then add all weighted scores. Maximum possible: 175. The total calculates automatically when you fill in scores.

0	Not scored
1 - 87	Do not engage - critical capability gaps
88 - 121	Below threshold - significant improvements needed
122 - 148	Meets requirements - acceptable candidate
149 - 175	Strong candidate - exceeds requirements

Red Team Provider Evaluation Criteria

#	Criterion	Weight	Score (1-5)
E1	CVE publication track record	High (3)	
E2	TLPT/TIBER prior experience	High (3)	
E3	Financial sector experience	High (3)	
E4	Live production system testing experience	High (3)	
E5	Operational security maturity	High (3)	
E6	Kill switch and halt procedures	High (3)	
E7	AV/EDR/XDR bypass capability	High (3)	
E8	Social engineering methodology	Medium (2)	
E9	Physical security testing capability	Medium (2)	
E10	Report quality and depth of findings	High (3)	
E11	Communication and weekly reporting quality	Medium (2)	
E12	Team depth and replacement capacity	Medium (2)	
E13	ISO 27001 or equivalent ISMS	Medium (2)	
E14	Custom tooling and C2 infrastructure	High (3)	
E15	Collaboration with TI providers	Medium (2)	
E16	Provider rotation	Low (1)	
E17	Leg-up process experience	Medium (2)	
	WEIGHTED TOTAL (Max: 210)		

How to use. Rate each criterion from 1 (poor) to 5 (excellent). Multiply each score by the weight number in parentheses, then add all weighted scores. Maximum possible: 210. The total calculates automatically when you fill in scores.

0	Not scored
1 - 104	Do not engage - critical capability gaps
105 - 146	Below threshold - significant improvements needed
147 - 177	Meets requirements - acceptable candidate
178 - 210	Strong candidate - exceeds requirements

04

Preparation Phase

Submit the project charter and scope specification to the TLPT Authority, coordinate with third-party providers, and complete cross-border arrangements.

Key deadline: Months 0-6 after notification

PLAN

Module 04: Preparation Phase

4A: Initiation (Within 3 Months of Notification)

- [ ] Control Team Lead name and contact details
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Tester type decision: internal / external / hybrid
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Communication channels: email encryption, data room, instant messaging
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] TLPT code name
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Critical functions in other Member States (list + jurisdictions)
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Critical functions supported by ICT third-party providers
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Expected completion deadlines for each phase
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Establish encrypted communication channels with TLPT Authority
  CRITICAL [RTS Art. 9(2); RTS Art. 4]
- [ ] Set up secure data room
  HIGH [RTS Art. 4]
- [ ] Confirm TLPT authority has validated initiation information
  CRITICAL [RTS Art. 9(3)]
- [ ] Confirm TLPT authority has validated control team composition
  CRITICAL [RTS Art. 9(5)]

4B: Scope Specification (Within 6 Months of Notification)

- [ ] List ALL identified critical/important functions
  CRITICAL [RTS Art. 9(6); RTS Annex II]
- [ ] For each CIF excluded: documented justification
  CRITICAL [RTS Art. 9(6); RTS Annex II]
- [ ] For each CIF included: rationale, ICT systems, outsourcing status, jurisdictions, flags
  CRITICAL [RTS Art. 9(6); RTS Annex II]
  - [ ] Inclusion rationale [RTS Annex II]
  - [ ] Supporting ICT systems identified [RTS Annex II]
  - [ ] Outsourcing status and provider identification [RTS Annex II]
  - [ ] Operating jurisdictions [RTS Annex II]
  - [ ] Preliminary flags (confidentiality, integrity, availability) [RTS Annex II]

- [ ] Management body formal approval obtained
  CRITICAL [RTS Art. 9(6)]

- [ ] Scope specification submitted to TLPT Authority
  CRITICAL [RTS Art. 9(6)]

- [ ] TLPT Authority approval received
  CRITICAL [RTS Art. 9(12)]

4C: Risk Assessment (Before Testing Starts)

- [ ] ICT risk assessment of the TLPT itself (RTS Article 5)
  CRITICAL [RTS Art. 5]

- [ ] Consider risks of: sensitive data access, compliance, incident escalation, production disruptions, blue team interference, incomplete restoration
  HIGH [RTS Art. 5]

- [ ] For pooled/joint TLPTs: additional multi-entity risk assessment
  CRITICAL [RTS Art. 6]

- [ ] Consult test managers on risk assessment before testing begins
  HIGH [RTS Art. 9(10)]

4D: Third-Party Provider Coordination

- [ ] Identify all ICT third-party providers supporting in-scope CIFs
  CRITICAL [DORA Art. 26(2); RTS Annex II]

- [ ] Review contracts for DORA Article 30(3)(d) cooperation clauses
  CRITICAL [DORA Art. 30(3)(d)]

- [ ] Amend contracts if cooperation clauses are missing
  CRITICAL [DORA Art. 30(3)(d)]

- [ ] Coordinate access arrangements with providers
  HIGH [DORA Art. 26(3)]

- [ ] Agree on risk management measures with providers
  HIGH [DORA Art. 26(5)]

- [ ] For pooled testing: coordinate with other financial entities
  HIGH [DORA Art. 26(4); RTS Art. 8]

- [ ] Confirm provider participation in writing
  HIGH [DORA Art. 26(3)]

4E: Cross-Border Coordination (If Applicable)

- [ ] Identify all Member States where in-scope CIFs operate
  CRITICAL [RTS Art. 16(1)]

- [ ] TLPT Authority notifies host Member State authorities
  CRITICAL [RTS Art. 16(1)]
- [ ] Host authorities respond within 20 working days
  HIGH [RTS Art. 16(1)]
- [ ] Agree on lead TLPT Authority
  CRITICAL [RTS Art. 16(1)]
- [ ] Negotiate mutual recognition conditions BEFORE testing begins
  CRITICAL [DORA Art. 26(7); RTS Art. 16]
- [ ] For group entities: assess whether joint TLPT is appropriate
  HIGH [RTS Art. 16(2)]

RED TEAM INSIGHT

Third-party coordination is the hidden time sink. Cloud providers and core banking vendors move slowly. Start contractual negotiations the moment you know they'll be in scope. This single item has been known to delay TLPTs by 3+ months.

RED TEAM INSIGHT

The contract amendment with your third-party ICT provider is where TLPTs go to die. Core banking vendors and cloud providers have their own legal teams, their own risk appetite, and their own timelines. Start this the day you know the provider is in scope.

RED TEAM INSIGHT

Failing to secure mutual recognition agreements before starting means you may end up running separate tests in each jurisdiction. Get this sorted during preparation, not after.

RED TEAM INSIGHT

Cross-border mutual recognition is not automatic even with the DORA attestation. Each host authority has 20 working days to decide whether they want to observe or participate. If you operate in three Member States, assume three sets of regulatory expectations to manage.

Key TLPT Risks (Pre-Populated Register)

Top 10 risks from the full 24-risk register. RTS Article 5 requires ICT risk assessment of the TLPT itself.

ID	Risk	Category	L	I	Score	Level
R-01	Production system disruption from red team tools	Operational	3	5	15	High
R-02	Residual red team artifacts post-testing	Operational	4	4	16	**Critical**
R-04	Unauthorized access to PII/customer data	Confidentiality	4	4	16	**Critical**
R-06	TLPT documentation leak	Confidentiality	2	5	10	High
R-08	Testing exceeds provider contract scope	Compliance	3	5	15	High
R-10	Blue team escalates to full incident response	Reputational	4	4	16	**Critical**
R-13	ICT provider refuses TLPT participation	Third-party	4	4	16	**Critical**
R-17	Incomplete CIF mapping	Scope	4	4	16	**Critical**
R-20	Control team secrecy breach	Personnel	4	4	16	**Critical**
R-22	Blue team blocks all C2/phishing infrastructure	Technical	3	3	9	Medium

05

Threat Intelligence

TI provider gathers intelligence, develops threat scenarios, and delivers the Targeted Threat Intelligence Report for TLPT Authority approval.

Key deadline: 4-6 weeks after scope approval

INTEL

Module 05: Threat Intelligence

5A: Threat Intelligence Gathering

- [ ] TI provider analyzes generic and sector-specific intelligence
  CRITICAL [RTS Art. 10(1)]
- [ ] TI provider identifies relevant cyber threats and vulnerabilities
  CRITICAL [RTS Art. 10(1)]
- [ ] TI provider gathers contextualized target intelligence
  CRITICAL [RTS Art. 10(1); RTS Annex III]
  - [ ] Employee credentials from breaches [RTS Annex III]
  - [ ] Lookalike domains [RTS Annex III]
  - [ ] Vulnerable exposed software/systems [RTS Annex III]
  - [ ] Employee information exploitable for social engineering [RTS Annex III]
  - [ ] Dark web data sales [RTS Annex III]
  - [ ] Internet/public network information [RTS Annex III]
  - [ ] Physical targeting information [RTS Annex III]
- [ ] TI provider identifies threat actor profiles most likely to target the entity
  CRITICAL [RTS Art. 10(2); RTS Annex III]

5B: Scenario Development

- [ ] TI provider develops broad set of candidate scenarios
  CRITICAL [RTS Art. 10(2)]
- [ ] Scenario selection meeting held (CTL + TI provider + test managers)
  CRITICAL [RTS Art. 10(3)]
- [ ] CTL selects minimum 3 scenarios based on TI recommendation, TM input, feasibility, and entity profile
  CRITICAL [RTS Art. 10(3)]
- [ ] Selected scenarios cover different threat actors and TTPs
  CRITICAL [RTS Art. 10(2)]
- [ ] Each scenario targets different critical functions
  CRITICAL [RTS Art. 10(2)]
- [ ] Mandatory coverage: at least one scenario targeting availability, one integrity, one confidentiality
  CRITICAL [RTS Art. 10(4); RTS Annex III]
- [ ] Maximum 1 scenario may be non-threat-led (scenario-X)
  HIGH [RTS Art. 10(4)]
- [ ] For pooled TLPTs: at least 1 scenario targets third-party provider systems
  CRITICAL [RTS Art. 10(4)]
- [ ] For joint TLPTs: at least 1 scenario targets intra-group systems
  CRITICAL [RTS Art. 10(4)]

5C: Targeted Threat Intelligence Report (TTIR)

- [ ] TI provider delivers TTIR per Annex III: scope, intelligence assessment, threat landscape, actor profiles, min 3 scenarios
  CRITICAL [RTS Art. 10(5); RTS Annex III]

- [ ] Control team reviews and submits TTIR to test managers
  CRITICAL [RTS Art. 10(6)]

- [ ] TLPT Authority approves TTIR
  CRITICAL [RTS Art. 10(6)]

- [ ] Approved TTIR shared with red team
  CRITICAL [RTS Art. 9(8)]

RED TEAM INSIGHT

Generic threat intelligence produces generic tests. If your TTIR reads like it could apply to any bank in Europe, it will produce scenarios that test your email gateway and nothing else. Push the TI provider to go deep on YOUR technology stack, YOUR geography, YOUR business model.

RED TEAM INSIGHT

Scenario selection is where scoping failures surface. A common mistake is approving three scenarios that all target the same critical function from different angles. Map scenarios to CIFs explicitly before approval.

06

Red Team Testing

Execute the red team test plan across minimum 12 weeks of active testing, managing leg-ups, detection events, and operational risk in real time.

Key deadline: Minimum 12 weeks active testing

ATTACK

Module 06: Red Team Testing

6A: Red Team Test Plan

- [ ] Testers prepare Red Team Test Plan (Annex IV) including communication, TTPs, risk measures, per-scenario details, attack paths, leg-ups, scheduling, infrastructure notes
  CRITICAL [RTS Art. 11(1); RTS Annex IV]
- [ ] Control team reviews and approves plan
  CRITICAL [RTS Art. 11(3)]
- [ ] TLPT Authority approves plan
  CRITICAL [RTS Art. 11(3)]

6B: Active Testing Execution

- [ ] Active red team testing begins
  CRITICAL [RTS Art. 11(4)]
- [ ] Duration minimum 12 weeks (proportionate to scope and complexity)
  CRITICAL [RTS Art. 11(5)]
- [ ] Scenarios execute sequentially or simultaneously per plan
  HIGH [RTS Art. 11(5)]
- [ ] Testers provide minimum weekly progress reports to control team and test managers
  CRITICAL [RTS Art. 11(7)]
- [ ] TI provider remains available for consultation throughout
  HIGH [RTS Art. 11(7)]
- [ ] All tester actions logged
  CRITICAL [TIBER-EU Section 5.2]

6C: Operational Management During Testing

- [ ] Control team monitors progress against plan
  HIGH [RTS Art. 4; RTS Art. 11(6)]
- [ ] Leg-ups provided as needed: each documented with code, type, reason; approved by CTL and TM
  CRITICAL [RTS Art. 11(8)]
- [ ] If blue team detects activity: CTL proposes continuation measures to TM
  HIGH [RTS Art. 11(9)]
- [ ] Any plan changes require CTL and TM approval
  CRITICAL [RTS Art. 11(6)]
- [ ] CTL may suspend TLPT if risk to data, assets, or services
  CRITICAL [RTS Art. 11(10)]

- [ ] Limited purple teaming as last resort (counts toward 12-week minimum)
  HIGH [RTS Art. 11(10)]

- [ ] TM validation required for limited purple teaming
  CRITICAL [RTS Art. 11(10)]

RED TEAM INSIGHT

Define your leg-up process before day one of active testing, not when the red team is stuck at week four. Pre-agree the categories, who approves them, the maximum response time (48 hours is a reasonable target), and what documentation is required.

RED TEAM INSIGHT

The 12-week minimum is real. Attempts to compress this timeframe consistently fail - regulators push back. Budget for 12-16 weeks of active testing.

RED TEAM INSIGHT

Kill switch decision paralysis is a real phenomenon. Pre-designate exactly one person with authority to halt the test immediately, and one person (different) with authority to resume it. Both should be reachable 24/7 during active testing.

07

Closure Phase

Blue team notification, red team and blue team reporting, mandatory purple teaming, 360-degree feedback, and test summary report submission.

Key deadline: Up to 18 weeks post-testing

REPORT

Module 07: Closure Phase

7A: Blue Team Notification

- [ ] Active testing ends (all parties agree)
  CRITICAL [RTS Art. 11(5)]
- [ ] Control team lead informs blue team that a TLPT took place
  CRITICAL [RTS Art. 12(1)]
- [ ] Blue team receives red team test report (may be cleared of sensitive information)
  HIGH [RTS Art. 12(3)]

7B: Reporting (Strict Deadlines)

- [ ] Red Team Test Report (Annex V) - within 4 weeks of active testing end
  CRITICAL [RTS Art. 12(2)]
  - [ ] Targeted CIFs and supporting systems [RTS Annex V(a)]
  - [ ] Per-scenario summary [RTS Annex V(a)]
  - [ ] Reached and unreached flags [RTS Annex V(a)]
  - [ ] Successful and unsuccessful attack paths and TTPs [RTS Annex V(a)]
  - [ ] Plan deviations (if any) [RTS Annex V(a)]
  - [ ] Leg-ups granted (if any) [RTS Annex V(a)]
  - [ ] Blue team actions detected by testers [RTS Annex V(b)]
  - [ ] Vulnerability descriptions with criticality ratings [RTS Annex V(c)]
  - [ ] Root cause analysis of successful attacks [RTS Annex V(c)]
  - [ ] Remediation recommendations with priority [RTS Annex V(c)]
- [ ] Red Team Report submitted to control team and test managers
  CRITICAL [RTS Art. 12(2); RTS Art. 12(3)]
- [ ] Blue Team Test Report (Annex VI) - within 10 weeks of active testing end
  CRITICAL [RTS Art. 12(4)]
  - [ ] For each attack step: detected actions and corresponding log entries [RTS Annex VI]
  - [ ] Assessment of tester findings and recommendations [RTS Annex VI]
  - [ ] Blue team-collected attack evidence [RTS Annex VI]
  - [ ] Blue team root cause analysis [RTS Annex VI]
  - [ ] Lessons learned and improvement potential [RTS Annex VI]
  - [ ] Purple teaming topics list [RTS Annex VI]
- [ ] Blue Team Report submitted to testers and test managers
  CRITICAL [RTS Art. 12(4)]

7C: Purple Teaming (Mandatory)

- [ ] Replay exercise: blue and red teams walk through attack and defense actions
  CRITICAL [RTS Art. 12(5)]
- [ ] Purple teaming on jointly identified topics
  CRITICAL [RTS Art. 12(5); TIBER-EU PT Guidance]
  - [ ] Tabletop discussion of alternative scenarios [TIBER-EU PT Guidance]
  - [ ] Re-exploration of attack scenarios on live systems [TIBER-EU PT Guidance]
  - [ ] Alternative scenario exploration on live systems [TIBER-EU PT Guidance]
  - [ ] Proof-of-concept development for untested vectors [TIBER-EU PT Guidance]
  - [ ] Discussion of anticipated remediation measures [TIBER-EU PT Guidance]
  - [ ] Business continuity exercise scenarios [TIBER-EU PT Guidance]
- [ ] All parties exchange feedback
  CRITICAL [RTS Art. 12(6)]
- [ ] Test managers may provide feedback
  MEDIUM [RTS Art. 12(6)]
- [ ] 360-degree feedback session conducted
  HIGH [RTS Art. 12(6); TIBER-EU Section 6.3]

7D: Test Summary Report (Annex VII)

- [ ] Involved parties documented
  CRITICAL [RTS Art. 12(7); RTS Annex VII(a)]
- [ ] Project plan documented
  CRITICAL [RTS Annex VII(b)]
- [ ] Validated scope with CIF rationale
  CRITICAL [RTS Annex VII(c)]
- [ ] Selected scenarios and TTIR deviations
  CRITICAL [RTS Annex VII(d)]
- [ ] Executed attack paths and TTPs used
  CRITICAL [RTS Annex VII(e)]
- [ ] Captured and non-captured flags
  CRITICAL [RTS Annex VII(f)]
- [ ] Red team test plan deviations (if any)
  CRITICAL [RTS Annex VII(g)]
- [ ] Blue team detections
  CRITICAL [RTS Annex VII(h)]
- [ ] Purple teaming conducted (if during testing phase)
  CRITICAL [RTS Annex VII(i)]

- [ ] Leg-ups documented
  CRITICAL [RTS Annex VII(j)]
- [ ] Risk management measures taken
  CRITICAL [RTS Annex VII(k)]
- [ ] Vulnerabilities with criticality ratings
  CRITICAL [RTS Annex VII(l)]
- [ ] Root cause analysis of successful attacks
  CRITICAL [RTS Annex VII(m)]
- [ ] High-level remediation plan
  CRITICAL [RTS Annex VII(n)]
- [ ] Lessons learned from feedback
  HIGH [RTS Annex VII(o)]
- [ ] Submitted to TLPT Authority
  CRITICAL [RTS Art. 12(7); DORA Art. 26(6)]

RED TEAM INSIGHT

The way you brief the blue team sets the tone for everything that follows. Frame findings as 'here is what an attacker with nation-state resources achieved against your defenses' not 'here is what you missed.' The blue team's cooperation determines whether remediation addresses root causes or patches symptoms.

RED TEAM INSIGHT

Purple teaming is where the real value is. The red team operation reveals gaps - but purple teaming transfers knowledge to your defenders.

RED TEAM INSIGHT

Purple teaming is not a debrief with slides. It is a hands-on technical exercise. The most effective sessions involve the blue team sitting with the red team, replaying attack paths in real time. If your plan is a two-hour meeting with a PowerPoint, you are leaving 80% of the value on the table.

08

Remediation & Attestation

Document remediation measures for every finding, submit to the TLPT Authority, and receive the formal attestation confirming DORA compliance.

Key deadline: 8 weeks after test summary submission

ATTEST

Module 08: Remediation & Attestation

8A: Remediation Plan (Within 8 Weeks of TSR Notification)

- [ ] For EACH finding, document all required fields
  CRITICAL [RTS Art. 13(2)]
  - [ ] Shortcoming description [RTS Art. 13(2)(a)]
  - [ ] Proposed remediation measures with prioritization [RTS Art. 13(2)(b)]
  - [ ] Completion timeline and milestones [RTS Art. 13(2)(b)]
  - [ ] Root cause analysis [RTS Art. 13(2)(c)]
  - [ ] Responsible staff/functions [RTS Art. 13(2)(d)]
  - [ ] Risk assessment if NOT remediated [RTS Art. 13(2)(e)]
  - [ ] Risk assessment of remediation implementation itself [RTS Art. 13(2)(e)]
- [ ] Remediation plan submitted to TLPT Authority AND competent authority (if different)
  CRITICAL [RTS Art. 13(1)]
- [ ] Follow-up oversight process established
  HIGH [DORA Art. 26(6)]

8B: Attestation

- [ ] TLPT Authority confirms all reports contain required information
  CRITICAL [RTS Art. 14; DORA Art. 26(7)]
- [ ] Attestation issued (Annex VIII) containing: test dates, CIFs, entities, providers, tester info, duration, authorities, documents
  CRITICAL [RTS Art. 14(1); RTS Annex VIII]
- [ ] For cross-border: attestation shared with relevant authorities for mutual recognition
  CRITICAL [RTS Art. 16(1); DORA Art. 26(7)]
- [ ] Next TLPT cycle planning begins (due within 3 years)
  HIGH [DORA Art. 26(1)]

RED TEAM INSIGHT

The most common remediation failure: the plan addresses the specific vulnerability instead of the systemic weakness. If a service account with a weak password was compromised, the fix is not 'change that password.' The fix is 'implement privileged access management across all service accounts.'

RED TEAM INSIGHT

Every finding needs an honest risk assessment for the scenario where remediation is delayed. Regulators do not expect 100% remediation in 8 weeks. They expect a credible plan with realistic timelines.

RED TEAM INSIGHT

Data destruction after a TLPT is not optional and it is not a formality. Your contract should specify destruction timelines (30 days post-attestation is a reasonable target), destruction methods (cryptographic erasure), and a signed destruction certificate from every external provider.

National TLPT Implementation Comparison

Status of TIBER-EU / DORA TLPT implementation across 32 jurisdictions. Last updated March 2026.

Country	TLPT Authority	Framework	Status	Internal Testers
EU/ECB (SSM)	ECB	TIBER-EU / SSM Guide	Operational	No (external only)
Austria	OeNB + FMA	TIBER-AT	Operational	Per RTS rules
Belgium	NBB	TIBER-BE	Operational	Per RTS rules
Czech Republic	CNB	TIBER-CZ	Operational	Per RTS rules
Denmark	Danish FSA + Nationalbank	TIBER-DK	Operational	Per RTS rules
Finland	FIN-FSA + Bank of Finland	TIBER-FI	Operational	Per RTS rules
France	Banque de France	TIBER-FR	Operational	Per RTS rules
Germany	BaFin + Bundesbank	TIBER-DE	Operational	Per RTS rules
Iceland	Sedlabanki	TIBER-IS	Operational	Per RTS rules
Ireland	Central Bank of Ireland	TIBER-IE	Operational	Per RTS rules
Italy	Banca d'Italia + CONSOB + IVASS	TIBER-IT	Operational	Per RTS rules
Liechtenstein	FMA LI	TIBER-EU LI	Operational	Per RTS rules
Luxembourg	CSSF + BCL	TIBER-LU	Operational	Per RTS rules
Malta	MFSA	TIBER-MT	Operational	Per RTS rules
Netherlands	DNB	TIBER-NL / ART	Operational	Per RTS rules
Norway	Norges Bank + Finanstilsynet	TIBER-NO	Operational	Per RTS rules
Portugal	Banco de Portugal	TIBER-PT	Operational	Per RTS rules
Romania	BNR	TIBER-RO	Operational	Per RTS rules
Slovakia	NBS	TIBER-SK	Operational	Per RTS rules
Spain	BdE + CNMV + DGSFP	TIBER-ES	Operational	Per RTS rules
Sweden	Sveriges Riksbank	TIBER-SE	Operational	Per RTS rules
Bulgaria	BNB	No national framework	DORA applies directly	Per RTS rules
Croatia	HNB + HANFA	No national framework	DORA applies directly	Per RTS rules
Cyprus	CBC + CySEC	No national framework	DORA applies directly	Per RTS rules

Country	TLPT Authority	Framework	Status	Internal Testers
Estonia	Finantsinspektsioon	No national framework	DORA applies directly	Per RTS rules
Greece	Bank of Greece	No national framework	DORA applies directly	Per RTS rules
Hungary	MNB	No national framework	DORA applies directly	Per RTS rules
Latvia	Latvijas Banka	No national framework	DORA applies directly	Per RTS rules
Lithuania	Lietuvos bankas	No national framework	DORA applies directly	Per RTS rules
Poland	KNF + NBP	TIBER-PL (planned)	In development	Per RTS rules
Slovenia	Banka Slovenije	No national framework	Transposition delayed	Per RTS rules
United Kingdom	BoE / PRA / FCA	CBEST + STAR-FS	Operational (independent)	Framework-specific

Operational Published / In development Delayed

afine
digitally secure

About AFINE

AFINE provides offensive information security services, specializing in penetration testing, security audits, and Red Team operations.

Our research team has published over 150 CVEs across SAP, Microsoft, IBM, CyberArk, Check Point, F5, Rapid7, Palo Alto Networks, and Adobe. That research output is what makes the difference in a TLPT - finding vulnerabilities that scanners and standard pentests miss.

150+	10	ISO 27001
PUBLISHED CVES	YEARS OPERATING	CERTIFIED

> "AFINE keeps finding critical issues where other pentesters have not found them."
>
> - Isabel Group

Team certifications: OSCP (minimum per researcher), OSCE, OSWE, OSED, OSEP, CRTO, CSSA, CISSP, CISA, BSCP

Reference clients: PKO BP, ING Bank, BGK, CPBiI, BIK, Tpay, BPS, Altira

Contact
afine.com | pwoyke@afine.com

Ready to start your TLPT journey?

Book a TLPT consultation

AFINE sp. z o.o.
pwoyke@afine.com