Digital Operational Resilience Testing

*Part 4 of the **DORA Deep Dive** Series*

Presented By:

Gerard Joyce, CTO, CalQRisk

Tuesday 10th December 2024

Outline

- Introductions
- DORA Overview
- Digital Operational Resilience Testing(What's in the Act)
- What elements apply to whom?
- Draft Regulatory Technical Standards (JC 2024-29)
- Basic
- Advanced
- Q&A

Who we are and what we do

- Experienced Risk & Compliance Professionals
- Members of IRM, IOB, CI (ACOI), IoD, ACCA, ISACA, ….
- We Make A Governance, Risk & Compliance Solution called CalQRisk
  - A cloud-based software solution
  - Includes a DORA-specific solution (Checklists / Register of Information report..)
- Risk Advisory Service
  - In-house / Virtual Training, Strategic Risk Alignment, Risk Management Framework development
- CalQRisk is used by 3,000+ users in regulated firms and others

  Including: Financial Services organisations and Not-For-Profit sector / Public Sector

66

Only those who dare to fail greatly, can ever achieve greatly

Robert F. Kennedy

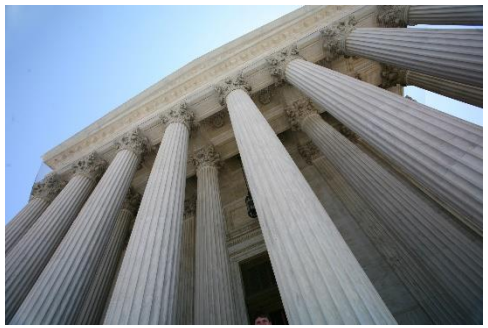
99

DORA Overview

- A Regulation. Applies to all EU Member States
- Came into force in Jan 2023
- It becomes applicable on Jan 17th 2025
- Applies to financial entities and some of their service providers
- It's about making the ICT systems that support financial business better
- Better in the sense that they are more secure, less likely to fail, faster to get back up and running, if they do fail.
- It harmonises and improves several guidelines that are in operation today.

DORA closes a gap by ensuring that operational resilience is not merely about financial buffers

DORA Five Pillars



- ICT Risk Management Framework - Oct 15th
- ICT Third Party Risk Management - Nov 12th
- ICT-related Incident Management - Nov 26th
- **Digital Operational Resilience Testing - Dec 10th Today**
- Information Sharing Arrangements- Jan 14th

Definitions

‘**threat-led penetration testing** (TLPT)’

means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity’s critical live production systems;

Digital Operational Resilience Testing (Act)

- **Article 11:** Response and recovery. (includes … periodically test ICT business continuity plans, crisis communication. Review policy, taking results of test into account)
- **Article 12:** Backup policies and procedures, restoration and recovery procedures and methods (Test backup procedure periodically)
- **Article 15:** Further harmonisation of ICT risk management tools, methods, processes and policies (ESA to develop RTS)

Digital Operational Resilience Testing (Act)

Digital Operational Resilience Testing – Chapter IV

- **Article 24:** General requirements for the performance of digital operational resilience testing

  (Maintain testing programme as part of RM framework, programme to include a range of tests, risk-based approach, tests undertaken by independent parties, policies and procedures to classify and remedy identified weaknesses, conduct, at least annually, tests on all critical systems / applications)

- **Article 25:** Testing of ICT tools and systems

  (Vulnerability assessments and scans, open source analyses, network security assessments, physical security, questionnaires and scanning software solutions, source code reviews, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing)

- **Article 26:** Advanced testing of ICT tools, systems and processes based on TLPT

  (every 3 years, all critical or important functions, identify ICT systems, include ICT TPs, pooled testing allowed, provide summary of findings and remediation plans to CA, **ESAs to develop RTS**)

- **Article 27:** Requirements for testers for the carrying out of TLPT

  (competent, ethical, sound risk management, have PII. Where internal: independent, approved, no CoI, Threat intelligence provider is extn)

Digital Operational Resilience Testing

The Who

Regulatory Technical Standards (JC 2024-29)

- **Article 2**: *Identification of financial entities required to perform TLPT*
  - *Credit institutions identified as global systemically important institutions*
  - *Payment institutions, exceeding in each of the previous two financial years EUR 150 billion of total value of payment transactions*
  - *Electronic money institutions, exceeding in each of the previous two financial years EUR 150 billion of total value of payment transactions*
  - *Central securities depositories;*
  - *Central counterparties;*
  - *Trading venues with an electronic trading system that meet at least one of several criteria*
  - *Insurance and reinsurance undertakings that meet all certain criteria (eg. GWP > €1,500,000,000)*

Regulatory Technical Standards (JC 2024-29)

- ***For those not in scope for TLPT.***
- *See Article 24 of DORA*

Digital Operational Resilience Testing

The How

Digital Operational Resilience Testing (Act)

Article 24: General requirements for the performance of digital operational resilience testing

- Maintain a sound and comprehensive DOR testing programme as an integral part of the ICT risk-management framework
- Include a range of assessments, test, methodologies, practices and tools. (See Articles 25 / 26)
  - (Vulnerability assessments /scans, open source analyses, network security assessments, physical security, questionnaires, source code reviews, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing)
- Follow a risk-based approach
- Tests are undertaken by independent parties (can be internal), avoid conflicts of interest
- Establish policies and procedures to prioritise, classify and remedy all issues revealed in tests. And validate fixes.
- Conduct tests, at least annually on all ICT systems and applications supporting critical or important functions.

Regulatory Technical Standards (JC 2024-29)

Mandate – Article 26(11) of DORA

The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:

1. *the criteria used for the purpose of the application of paragraph 8, second subparagraph*1;

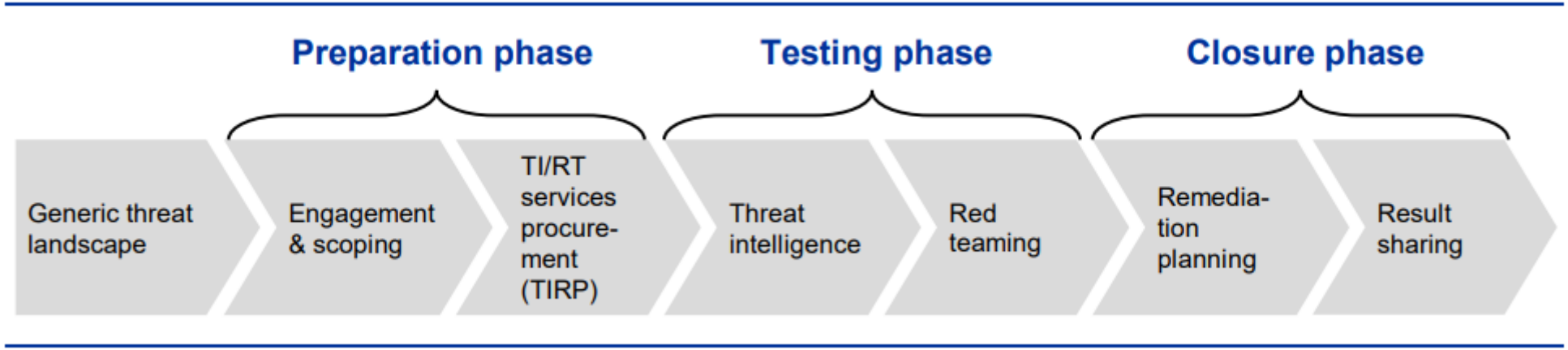
2. *the requirements and standards governing the use of internal testers;*

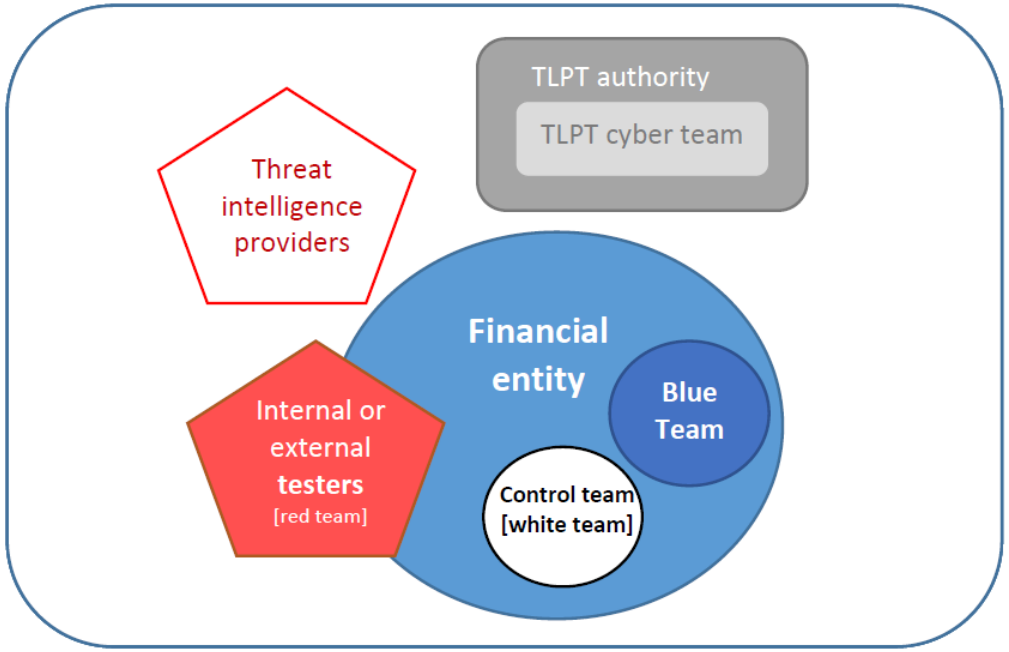
3. *the requirements in relation to:*
   (i) the scope of TLPT referred to in paragraph 2;
   (ii) the testing methodology and approach to be followed for each specific phase of the testing process;
   (iii) the results, closure and remediation stages of the testing;

4. *the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.*

When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.

TIBER-EU Process





Regulatory Technical Standards (JC 202429)

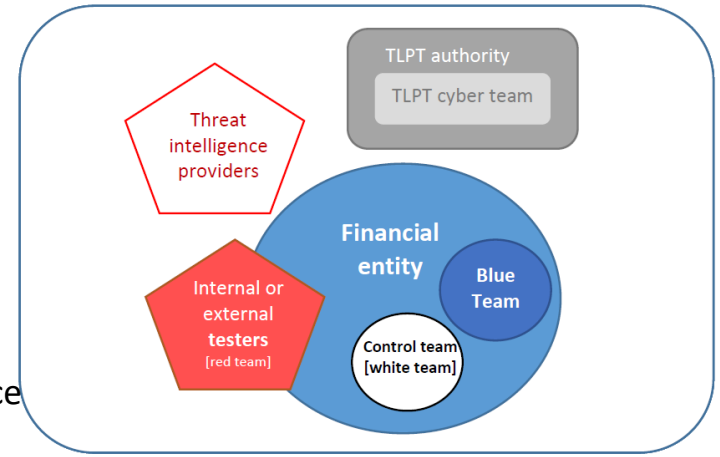
TESTING METHODOLOGY

- **Article 3**: **TCT and TLPT Test Managers**
  - Authority will assign TLPT-related activities to a TCT (TLCT Cyber Team)
  - Test manager will be designated.. For each test, Test managers will ensure compliance with requirements
  - TLPT authority shall participate in all phases of the TLPT
- **Article 4**: **Organisational arrangements for financial entities**
  - FEs shall appoint a “control team”
  - FEs shall establish organisational and procedural measures covering: access to information, liaison with test manager, informing the CT of any detection and then limiting escalation, keeping secrecy of the TLPT.
- **Article 5**: **Risk management for TLPT**
  - Assess risks of testing live system & Manage risks (certification of testers, PII in place, references, skill and qualifications,
  - Consider risks of granting access to sensitive information
  - Carry out restoration procedures at the end of the test
- **Article 6: Risk management for pooled and joint TLPTs**
  - Each control team to conduct own risk assessments and consider risk associated with the involvement of other FEs

Regulatory Technical Standards (JC 202429)

TESTING PROCESS

- **Article 7: Specificities for pooled and joint TLPTs**
  - Each FE to follow steps in Article 8-13
  - TLPT authority = lead TLPT authority
- **Article 8: Preparation phase**
  - FEs to submit a "project charter" to TLPT authority within 3 months of notice
  - FEs setup a "control team" once plan approved. Submit scope …
  - FE procure testers, consult test managers, assess compliance of testers and TI providers
- **Article 9: Testing phase: Threat Intelligence**
  - TI provider identifies relevant threats and vulnerabilities, proposes appropriate scenarios
  - Control team to select three scenarios, taking input from test manager into account, feasibility, own context,..
  - TI provider to provide targeted threat intelligence report to control team (Annex III), who shall submit to the test manager for approval



Regulatory Technical Standards (JC 202429)

TESTING PROCESS

- **Article 7: Specificities for pooled and joint TLPTs**
  - Each FE to follow steps in Article 8-13
  - TLPT authority = lead TLPT authority
- **Article 8: Preparation phase**
  - FEs to submit a "project charter" to TLPT authority within 3 months
  - FEs setup a "control team" once plan approved. Submit scope …
  - FE procure testers, consult test managers, assess compliance of test
- **Article 9: Testing phase: Threat Intelligence**
  - TI provider identifies relevant threats and vulnerabilities, proposes
  - Control team to select three scenarios, taking input from test mana
  - TI provider to provide targeted threat intelligence report to control anager for approval

ANNEX I

Content of the project charter

Item of information	Information required
Person responsible for the project plan, i.e. the Control Team Lead	Name Contact details
Testers	☐ internal ☐ external ☐ both
Communication channels selected in accordance with Article 8(1) point d) and 8(2) point a, including: (a) Email encryption to be used (b) Online data rooms to be used (c) Instant messaging to be used	
Codename for the TLPT	
If any, critical or important functions the financial entity operates in other Member States	1. List of critical or important functions operated in another Member State 2. for each critical or important function, indication of the Member State or States in which they are operated
If any, critical or important functions supported by ICT third party service providers	3. List of critical or important functions supported by ICT third-party service providers 4. for each function, identification of the ICT third party service provider
Expected deadlines for the completion of the:	
(1) Preparation Phase, in accordance with Article 8	yyyy-mm-dd
(2) Testing Phase, in accordance with Articles 9 and 10	yyyy-mm-dd
(3) Closure Phase, in accordance with Article 11	yyyy-mm-dd
(4) Remediation plan in accordance with Article 12	yyyy-mm-dd

Regulatory Technical Standards (JC 202429)

TESTING PROCESS

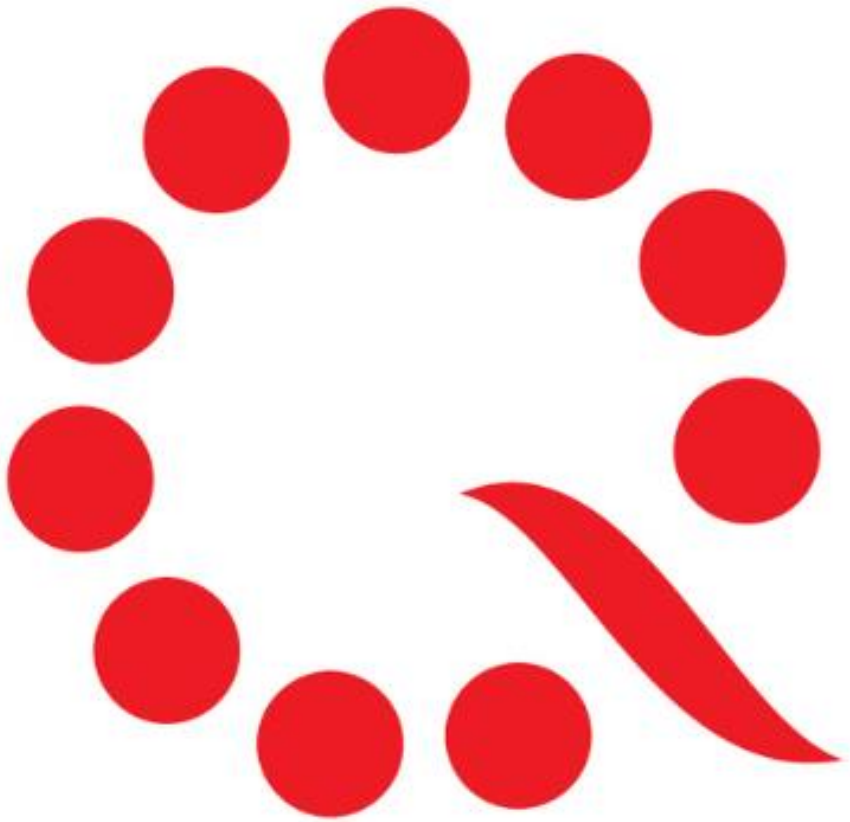
- **Article 10**: **Testing phase: Red Team Test**
  - Red Team to prepare test plan, using annex IV and scope docs
  - Testers to consult with TI provider, test manager on various aspects
  - Control team to approve plan, then test, report weekly, must keep secret, suspend if causing damage
- **Article 11**: **Closure phase**
  - Control team to inform blue team it was a TLPT test
  - Testers to submit report within 4 weeks to control team, who will provide to the blue team and test managers
  - Blue team will provide their test report withing 10 weeks of receiving Red Team report, showing what they detected…
  - Purple team to conduct exercise, all teams provide feedback to each other. FE has 8 weeks to submit report to authority
- **Article 12**: **Remediation Plan**
  - FE to provide remediation plans withing 8 weeks, incl. shortcomings, proposed remediation measure, priority, expected completion..
  - Also: root cause, who is responsible for remediation measures, risks associated with not implementing / implementing measures
- **Article 13: Use of internal testers**
  - Have policy, resources, capabilities, mention in reports, intra-group ARE internal.

Takeaways

- If you are one of the chosen few (under Art 2), you have a lot of work ahead of you.

For all others:….

- Read Article 24
  - Have a testing programme
- Keep aware of what threats and vulnerabilities apply to you
  - Gather Threat Intelligence, act on it
- Test a restore of your backup
- Just over 1 month to go (to Jan 17, 2025) !!



Questions ?

gerard.joyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk