CMAGE

Cyber Security Maturity Assessment Global Ecosystem

CREST

Government

Good Practice Guide

Fostering Financial Sector Cyber Resilience in Developing Countries

March 2023

Fostering Financial Sector Cyber Resilience in Developing Countries

Contents

Executive Summary

Ongoing digitalisation in the financial sector in recent years has seen considerable take-up of financial inclusion - embarking less-privileged people into the financial system and giving them access to credit, savings and payment services.

However, recent studies show cyber resilience of financial entities in developing countries is often relatively low, leaving them and their clients considerably exposed to cyber risks. Therefore, authorities in developing countries have stepped up their efforts to improve financial sector cyber resilience. One common element being considered in the respective cyber resilience strategies is testing - more specifically, Threat Led Penetration Testing.

Threat Led Penetration Testing (TLPT, or Intelligence-Led Red Team testing) is a controlled attempt to compromise the cyber resilience of an entity by simulating the behaviour (i.e. the tactics, techniques and procedures) of real-life threat actors, by making use of ethical hackers and targeted threat intelligence collected for this purpose.

TLPT is especially suited for entities that play a key role in the financial system and/or real economy and should only be applied to financial entities which are ready for it. These are entities which are relatively “cyber mature”.

They have basic cyber risk controls in place (also called basic “cyber hygiene”) and implemented relatively sophisticated risk mitigation measures in risk management domains such as governance, identification, protection, detection and recovery.

Less cyber mature entities should limit themselves to vulnerability assessments, penetration tests and scenario-based tests first, before undertaking this higher form of testing.

“One common element being considered in the respective cyber resilience strategies is testing - more specifically, Threat Led Penetration Testing."

Executive Summary

Threat Led Penetration Tests harbour elements of risk, owing to the criticality of the target systems, people and processes involved in the test, highlighting the need for active and robust risk management. One element of such risk management is the quality of the Threat Intelligence and Red Team service providers and their respective personnel.

So, a careful selection process is crucially important to the success of a TLPT test and for continuity of the respective financial entity.

An independent, not-for-profit accreditation and certification initiative - like CREST - can help financial entities and authorities alike in ensuring this much-needed high quality.

CREST builds trust in the digital world by raising professional standards and delivering measurable quality assurance for the global cyber security industry. By taking a collaborative approach and expressing the expectation that threat intelligence and Red Team service providers have CREST accreditation and cyber security professionals have CREST certification, a financial authority can contribute to a more mature market for cyber security services in its respective jurisdiction, benefiting all.

Executing a TLPT programme is a long-lasting endeavour. Not only because the threat intelligence led Red Team tests on the eligible financial entities take time, but also the capacity constraints at the authority in charge and the limited number of qualified threat intelligence and Red Team service providers mean few tests can take place at the same moment.

Next to that, threat led penetration testing is about learning and evolving; it is not meant to be a one-off exercise.

The paper concludes that if authorities - after careful consideration - pursue a Threat Led Penetration Testing programme, it will not only facilitate the improvement of cyber resilience of its most critical financial entities, it will also contribute to the maturing of the local market for cyber security services, benefiting other non-critical companies and society at large as well.

For the sake of common interest, achieving this objective requires close and constructive collaboration between all parties, private and public.

"An independent, not-for-profit accreditation and certification initiative - like CREST - can help financial entities and authorities alike in ensuring this much-needed high quality. CREST builds trust in the digital world by raising professional standards and delivering measurable quality assurance for the global cyber security industry."

Introduction

February 2016 was a watershed moment in thinking about cyber security and cyber resilience. Although on the agenda for years, the partly successful cyber heist on the Central Bank of Bangladesh made financial institutions and financial authorities realise that efforts to prepare for, and to protect from, cyber-attacks needed to be stepped up considerably.

Global developments since 2016 have further underscored the need to improve the cyber resilience level of financial entities - and the whole financial sector. Large-scale rapid digitalisation of financial products and services and supply chain extension by increasing use of third-party entities, combined with geopolitical tensions, have provided even more opportunities and motivations for individual hackers, malicious insiders, organised crime groups and nation-states alike.

While this applies to all countries, developing countries have an additional element. Ongoing digitalisation in the financial sector has provided the opportunity for considerable improvements regarding financial inclusion, i.e. embarking less-privileged people into the financial system and giving them access to credit, savings and payment services.

Financial inclusion is a top priority among the international community since the G20 recognised it as one of the main pillars of the global development agenda in 2010.

"Between 2017 and 2021 alone, the average rate of account ownership in developing economies increased by another 8 percentage points, from 63 percent of adults to 71 percent of adults, increasing the number of banked adults with many millions."[1]

By 2030, two billion new users will store money and make payments on their phones. Many financial inclusion efforts rely on leapfrogging to digital financial services - and are changing the level and type of interdependencies of the financial system and tech companies.[2]

While this is clearly a success, it also has exposed the formerly unbanked to cyber risk. Any theft of their digital savings, malicious alteration of their data, or obstruction of the financial infrastructure in general, can affect the less-privileged hardest, directly endangering their businesses, families and possibly even their lives. However, recent studies show the level of cyber resilience of financial entities in developing countries is often relatively low,[3] leaving them and their clients considerably exposed.[4] Central banks and financial authorities have an important task in increasing the level of their financial sector's cyber resilience. Since 2016, many authorities have developed and implemented cyber resilience strategies, including operational guidelines and cyber resilience expectations focusing on individual entities; others - especially in developing countries - are stepping up.

> *"By 2030, two billion new users will store money and make payments on their phones."*

[1] The Global Findex Database 2021 (World Bank Group, 2022)

[2] FinCyber Strategy Project: Cybersecurity and Financial Inclusion (*Carnegie Endowment for International Peace).*

[3] See for example the results of the CMAGE Project, funded by the Bill and Melinda Gates Foundation.

[4] See Cyber Threats to the Financial Sector in Africa. (World Bank & SecAlliance March 2022) for an intelligence-led analysis of the current threat landscape for the financial-service sector across Africa.

Introduction

One common element being considered in cyber resilience strategies is Threat Led Penetration Testing. This paper describes in relatively general terms what Threat Led Penetration Testing is, what different frameworks exist and what these have in common.

More importantly, this paper clarifies that Threat Led Penetration Testing is to be applied only to relatively “cyber mature” financial entities.

So, we ask why that is - and how to define cyber maturity. What steps can be taken to achieve the appropriate level of cyber maturity?

To answer these questions, this paper interprets, relies upon and refers to documents and policies from several financial authorities.

"One common element being considered in cyber resilience strategies is Threat Led Penetration Testing."

Cyber Resilience and Cyber Maturity

1.0 Cyber Resilience and Cyber Maturity

1.1 Inherent Cyber Risk

Cyber resilience is an organisation's ability to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment, and by withstanding, containing and rapidly recovering from cyber incidents.[5]

An organisation with a relatively high level of cyber resilience capabilities is generally understood as relatively "mature".

Before defining what "cyber maturity" entails, you could say the more an organisation is exposed to cyber risk (its inherent cyber risk level), the more cyber mature this organisation needs to be to ensure its continuity.[6]

Generally speaking, a fully paper- and trust-based local micro-lending scheme will have a low inherent cyber risk level, if at all.

An established financial entity using highly complex digital technologies to deliver a myriad of products and services across multiple delivery channels will understandably have a high inherent cyber risk level.

To define which inherent cyber risk category a financial entity would fall into (low, medium or high), the business and operational aspects of a financial entity need to be taken into account.

These include:

- Technology being used
- Delivery channels in use
- Products and technology services offered
- Business size
- Organisational characteristics, and
- The entities' track record of cyber threats.

Financial entities of systemic importance for the financial system[7] automatically fall under the high inherent risk category, as in the event of their distress or failure, they could cause significant disruption to the financial system and the broader economy.

These financial entities should have the highest level of cyber maturity, and if they don't have it yet, they should strive for it.

Whether FinTech challenger banks and mobile payment service providers in developing countries fall into the category of medium or high inherent cyber risk, depends on the assessment.

These new actors - which often offer fully digital financial services, mostly via mobile channels - have contributed considerably to improvement in financial inclusion.

However, any issues regarding their confidentiality, integrity or availability have the potential to directly endanger their client's businesses, families and possibly even their lives.

---

[5] FSB Cyber Lexicon - November 2018.

[6] The concept of inherent risk assessment referred to in this chapter is an important element of the Cyber Resilience Assessment Framework (C-RAF) of The Hong Kong Monetary Authority (HKMA).

[7] In general this could include: payment systems, central securities depositories, central counterparty clearing house, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies, and any other incumbent and new service providers deemed critical for the functioning of the financial sector.

1.0 Cyber Resilience and Cyber Maturity

1.2 Assessing Cyber Maturity

To help organisations enhance their cyber resilience, standard setting initiatives have issued international standards and frameworks for IT Security controls, including:[8]

- The NIST Cybersecurity Framework
- ISO/IEC 27002:2022 standard on Information security, cybersecurity and privacy protection
- ISACA's COBIT 5
- The Information Security Forum's Standard of Good Practice for Information Security
- The Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool.

Based on these standards and frameworks, financial authorities have developed their own guidance, guidelines and expectations specifically aimed at financial entities.

Two good examples of frameworks include the Hong Kong Monetary Authority's Cyber Resilience Assessment Framework (C-RAF)[9] and the Cyber Resilience Oversight Expectations (CROE) developed by the European Central Bank and adopted by the World Bank under the Financial Inclusion Global Initiative.[10]

The novelty of both C-RAF and CROE is that these two frameworks distinguish three levels of cyber maturity, i.e. baseline/evolving, intermediate/advancing and advanced/innovating.

While C-RAF is more geared towards banks, the CROE is drafted with financial market infrastructures in mind. Nevertheless, both frameworks draw on the same principles and are to a certain level entity agnostic. They could be used by any financial entity and its respective authority to establish the **current** and **expected** level of cyber maturity.

[8] For further detail see: NIST Cybersecurity Framework, ISO/IEC 27002, ISACA's COBIT 5 framework, the information security forums Standard of Good Practise for Information Security, and the Federal Financial Institutions Examinations Council's (FFIEC) Cybersecurity Assessment Tool.

[9] C-RAF is part of the HKMA's Cybersecurity Fortification Initiative (originally launched in 2016 and updated in 2020), which is underpinned by three pillars: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP), and the Cyber Intelligence Sharing Platform (CISP).

[10] The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructure (CPMI), and the International Telecommunications Union (ITU) funded by the Bill & Melinda Gates Foundation to support and accelerate implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal.

1.0 Cyber Resilience and Cyber Maturity

1.2 Assessing Cyber Maturity

As the audience of this paper are authorities and financial entities from developing and emerging economies, the Cyber Resilience Oversight Expectations (CROE) - as adopted by the World Bank - are used as reference from now on.[11]

Three levels of Cyber Maturity:

i **Evolving level.** Essential capabilities are established and evolve, and are sustained across the financial entity, to identify, mitigate and manage cyber risks in alignment with the Board-approved cyber resilience strategy and framework, and performance of practices is monitored and managed.

ii **Advancing level.** In addition to meeting the Evolving level, practices incorporate more advanced implementations (e.g.: advanced technology and risk management tools) that are integrated across the financial entities business lines and have been improved over time to pro-actively manage cyber risks to the financial entity.

iii **Innovating level.** In addition to meeting Evolving and Advancing levels, capabilities across the financial entity are enhanced as needed in the midst of the rapidly evolving cyber threat landscape, in order to strengthen the cyber resilience of the financial entity and its ecosystem by pro-actively collaborating with its external stakeholders. The innovating level entails driving innovation in people, process and technology for the financial entity and wider ecosystem to manage cyber risks and enhance cyber resilience. This may entail developing new controls, new tools, or creating new information sharing groups.

Source: Cyber Resilience for Financial Market Infrastructures. (Page 9, World Bank / ECB Nov 2019)

1.2.1 Ensuring Basic Cyber Hygiene Implemented

Before engaging in any programme to improve the level of cyber maturity of a respective financial entity, the first step is to ensure basic steps and measures have been taken to deliver a minimal level of protection against threat actors. While the classification “evolving” is referred to as the lowest level of cyber maturity in the CROE,[12] even this classification implies several steps and measures have already been taken before even reaching that level.

To put it differently, basic cyber hygiene needs to be in place for any organisation having a digital presence. Supervisors and overseers are often confronted with financial entities which do not even have their basic cyber hygiene in order. This is confirmed by research executed in the context of the CMAGE project.[13]

[11] Cyber Resilience Oversight Expectations (ECB, December 2018) and Cyber Resilience for Financial Market Infrastructures (FIGI - World Bank, International Telecommunication Union, Gates Foundation and CPMI, November 2019).

[12] C-RAF refers to the lowest level as “baseline”.

[13] The CMAGE project provides insight in a country’s cyber posture. This includes a country’s banking sector, which is rated on a cyber maturity scale from 1 (low) to 5 (high) based on four indicators which capture the basic cyber controls: infrastructure vulnerability risk, architecture & access risk, email authentication risk, and information leakage risk. These four indicators relate to the primary risk management domain “protection” (see paragraph 1.2.2 of this chapter).

1.0 Cyber Resilience and Cyber Maturity

1.2 Assessing Cyber Maturity

Passive reconnaissance of the external (internet facing) digital parameters of many financial service providers[14] in several African and Asian countries reveals that often controls (such as boundary firewalls and internet gateways, malware protection, patch management, allow listing and execution control, secure configuration, password policy and user access control, for example) are not properly implemented.[15]

The consequences of bad basic cyber hygiene can be dire, and include:

- Breached credentials
- Phishing
- CEO fraud
- Open ports
- Unpatched software, and
- Expired certificates.

For example, resulting in the breach of confidentiality, integrity and/or availability of data and systems.

1.2.2 Aspiring to the Next Level of Cyber Maturity

Assuming a financial entity has successfully implemented the basic cyber risks controls mentioned above, it can embark on the process of assessing the current level of its cyber maturity and of defining - together with the relevant supervisory authority - the aspired and/or expected level.

Authorities (supervisors and overseers) measure the level of an entity's cyber resilience (its so-called "cyber maturity") along five primary risk management domains:

- Governance
- Identification
- Protection
- Detection
- Response & recovery.

And three additional overarching domains:

- Testing
- Situational awareness
- Learning & evolving.

To achieve resilience objectives, investments across these domains can be mutually reinforcing and should be jointly considered.[16] An entity's relative maturity in all these domains defines whether it is ready to engage in regulatory-driven Threat Led Penetration Testing exercises.

To achieve resilience objectives, investments across these domains can be mutually reinforcing and should be jointly considered.[17] An entity's relative maturity in all these domains defines whether it is ready to engage in regulatory-driven Threat Led Penetration Testing exercises.

14 E.g. retail and wholesale banks, sharia banks, micro-finance institutions, etc.

15 These seven basic cyber controls are taken as an example for this paper and form part of the Cyber Essentials, as defined by the UK government.

16 These five primary risk management domains and three additional overarching domains have found their way into the EU's Digital Operation Resilience Act (DORA). DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT-related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogeneous across all EU member states. The core aim is to prevent and mitigate cyber threats.

17 Guidance on cyber resilience for financial market infrastructures (CPMI-IOSCO, June 2016).

1.0 Cyber Resilience and Cyber Maturity

1.2 Assessing Cyber Maturity

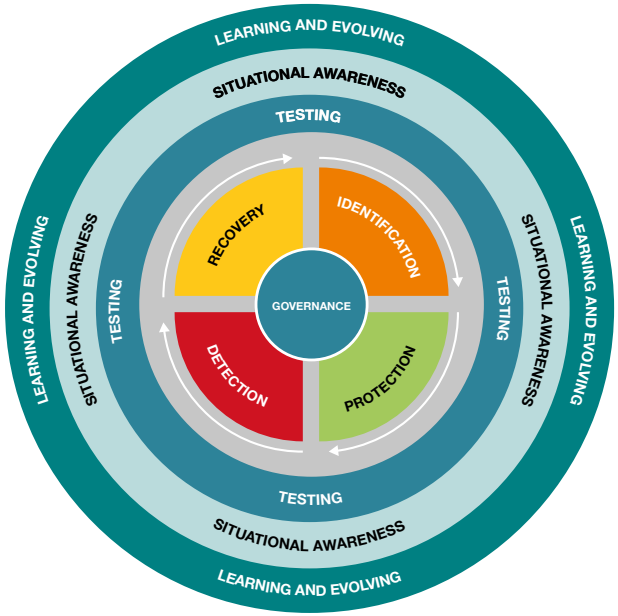


Figure1: Guidance on cyber resilience for financial market infrastructures (CPMI-IOSCO, June 2016)

The below summarises the key elements of the respective domains.[18]

Governance

Cyber governance refers to arrangements an entity has in place to establish, implement and review its approach to managing cyber risks.

Too often, cyber resilience has been delegated to the IT department, without a proper embedding of the topic into the wider strategy of the financial entity and without clearly defining the roles and responsibilities of management up to the level of the executive board. Effective cyber governance starts with a clear and comprehensive cyber resilience strategy and a more detailed framework that prioritizes the security and efficiency of the entity's operations.

The framework should define how the entity's cyber resilience objectives are determined, and outline its people, processes and technology requirements for managing cyber risks, including effectively responding to, and recovering from, cyber attacks.

It is essential the framework is supported by clearly defined roles and responsibilities of the Board and its management, and it is incumbent upon its Board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring the entity's cyber resilience. Strong cyber governance is essential to an entity's implementation of a systematic, proactive approach to managing any prevailing and emerging cyber threats it faces.

It also supports efforts to appropriately consider and manage cyber risks at all levels within the organization and to provide appropriate resources and expertise to deal with these risks.

Identification

Given a financial entity's operational failure can negatively impact its clients and even financial stability, it is crucial that such entities identify which operations and supporting information assets should be protected against compromise.

This must be done in order of priority, as 100% protection against cyber threats is not possible.

The ability of an entity to understand its internal situation and external dependencies is key to ensuring effective response to potential cyber threats.

This requires a financial entity to understand its information assets and processes, procedures, systems and all dependencies (including on third-party providers) to strengthen its overall cyber resilience posture.

18 Based on Cyber Resilience for Financial Market Infrastructures (FIGI - World Bank, International Telecommunication Union, Gates Foundation and CPMI, November 2019).

Protection

Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of a financial entity's assets and services. These measures should be proportionate to an entity's threat landscape and systemic role in the financial system, and consistent with its risk tolerance.

Financial entities should implement appropriate and effective measures in line with leading cyber resilience and cybersecurity practices to prevent, limit or contain the impact of a potential cyber event. The seven basic cyber controls mentioned earlier ("the basic cyber hygiene") fall mostly within this domain.

Detection

A financial entity's ability to recognise signs of a potential cyber incident, or detect that an actual breach has taken place, is essential to strong cyber resilience.

Early detection provides useful lead time to mount appropriate countermeasures against a potential breach. It also allows for proactive containment of actual breaches. Early containment could effectively mitigate the impact of the attack - for example, by preventing an intruder from gaining access to confidential data or ex-filtration of such data. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, a financial entity should maintain effective capabilities to extensively monitor for anomalous activities.

Response and Recovery

The ability of a financial entity to fulfil its obligations towards its clients and counterparts is crucial for its business continuity and - therefore - for financial stability.

It should be able to resume critical operations rapidly, safely and with accurate data, to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential for meeting related objectives.

Testing

Testing is an integral component of any cyber resilience framework, i.e. any structured plan to address the above-mentioned five risk management domains. All elements of a cyber resilience framework should be regularly and rigorously tested to determine their overall effectiveness. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the effectiveness of the cyber resilience framework in the financial entity and its environment is essential in determining the residual cyber risk to operations, assets and ecosystem.

Sound testing regimes produce findings that can then be used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the financial entity's cyber risk management process.

Analysis of test results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps.

Testing involves a range of activities starting at the level of rather basic vulnerability assessments, via penetration tests and scenario-based tests, up to high-end tests using external Red Teams guided by externally provided threat intelligence.[19]

19 These tests are called Threat Led Penetration Tests (TLPT) or Intelligence Led Red Teaming (ILRT) and driven by regulatory frameworks, including TIBER-EU (EU), CBEST (UK) or iCAST (Hong Kong).

1.2 Assessing Cyber Maturity

Situational awareness

Situational awareness refers to a financial entity's understanding of the cyber threat environment, the business implications of being in that environment, and the adequacy of its cyber risk mitigation measures.

Strong situational awareness, acquired through an effective cyber threat intelligence process, can make a significant difference in the ability to pre-empt cyber events or respond rapidly and effectively to them.

Keen appreciation of the threat landscape can help a financial entity better understand the vulnerabilities in its critical business functions and adopt appropriate risk mitigation strategies.

It can also enable a financial entity to validate its strategic direction, resource allocation, processes, procedures and controls with respect to building cyber resilience.

To achieve situational awareness, there needs to be active participation in information and intelligence-sharing initiatives and collaboration with trusted stakeholders in and outside the industry.[20]

Learning and Evolving

A financial entity's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment.

To keep pace with the rapid evolution of cyber threats, an adaptive cyber resilience framework should be adopted.

This framework needs to evolve with the dynamic nature of cyber risks and allows an organisation to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems.

A culture of cyber risk awareness should be instilled, whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

For each of the eight above-mentioned categories, more detailed expectations have been spelled out on the basis of which the financial entity and its supervisor could assess the current level of cyber maturity of that entity and define its expected (i.e. to be reached) level.

As a rule of thumb, all financial entities should meet the lowest (evolving) level and strive for the next level of cyber maturity (advancing). Financial entities of systemic importance to the financial sector and the wider economy should meet the expectations set for the medium (advancing) level and aim to achieve the highest (innovating) level as soon as possible.[21]

[20] For more information on the practical set-up and functioning of cyber information and intelligence sharing initiatives focusing on the financial sector, refer to the CIISI-EU initiative and its Irish equivalent CIISI-IE.

[21] For further details, see CROE or C-RAF documentation.

"A financial entity's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment. To keep pace with the rapid evolution of cyber threats, an adaptive cyber resilience framework should be adopted."

2.0 In Focus: Different Forms of Testing

2.0 In-Focus: The Different Forms of Testing

Ensuring the appropriate level of cyber resilience in an ever-changing organisational, technological and threat environment requires testing risk mitigation measures taken by the respective entity.

In general, there are four basic forms of testing:

- Vulnerability assessment
- Penetration testing
- Scenario-based (desk-top) testing, and
- Threat Led Penetration Testing (TLPT).[22]

While they differ in complexity, approach and intrusiveness, they all have their own advantages.

Vulnerability Assessment

Vulnerability Assessment - and with it, vulnerability scanning - is the simplest form of IT security testing. A vulnerability assessment is a systematic examination of an information system, its controls and processes, to determine the adequacy of security measures. It will identify security deficiencies, provide data to help predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.[23]

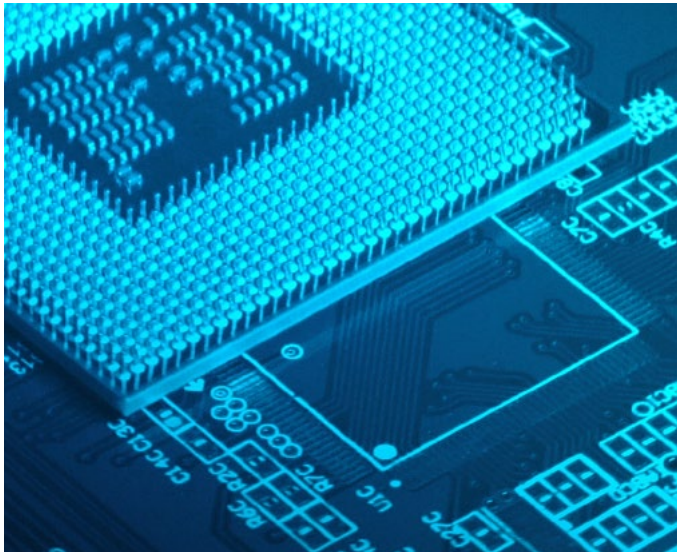
There are different types of vulnerability assessments, e.g. network-based assessments, host-based assessments, application assessments and database assessments.

Vulnerability scans - as part of vulnerability assessments - are predominately executed in a fully automated way, identifying publicly known vulnerabilities and misconfiguration in a single system.

A comprehensive vulnerability assessment evaluates whether an IT system is exposed to known vulnerabilities, assigns severity levels to identified vulnerabilities, and recommends remediation or mitigation steps where required.

Vulnerability assessment - and especially vulnerability scanning - is part of the basic cyber hygiene measures any organisation with a digital presence should have implemented.[24]

Depending on the expected - or aspired - level of cyber maturity, it should be performed on a regular to continuous basis, up to system and organisation wide.



[22] Following definitions used by regulatory authorities, this paper uses the term Threat Led Penetration Testing (TLPT) for tests which mimic real threat actors and simulate real attacks. However, a term like “Intelligence Led Red-teaming” (ILRT) would provide a more accurate understanding and a clearer distinction from normal penetration testing.

[23] See FSB Lexicon (FSB, November 2018).

[24] Under the earlier mentioned CMAGE project (see footnote 12), a country’s banking sector cyber posture is established by performing a vulnerability assessment on those elements of an entity’s IT infrastructure which are directly connected to the internet.

2.0 In-Focus: The Different Forms of Testing

Penetration Testing

Penetration Testing (or pen-testing) is a test methodology in which assessors, using all available documentation (system design, source code and manuals, for example) and working under specific constraints, attempt to circumvent the security features of an information system.[25]

Penetration tests provide a detailed and useful assessment of technical and configuration vulnerabilities, often within a single system or environment.

Next to vulnerability assessments and penetration testing comes scenario-based testing. While vulnerability assessments and penetration tests mainly focus on the technical side, scenario-based testing is more focused on the "soft" side of the organisation, its staff and its decision-making processes.

Scenario-based Testing

Scenario-based Testing is a desktop or simulation exercise, in which relevant board members and other senior managers are actively involved and have to answer questions like "what would you do if…". While "walking and talking" through carefully prepared, extreme but plausible scenarios, an entity's internal skills, processes and procedures are tested, with a view to achieving stronger operational resilience.

While vulnerability assessments, penetration tests and scenario-based tests are useful in their own right and "must-do's" for any entity which relies on information systems for its activities, they do not mimic the real physical and online world in which an entity is active.

Both vulnerability scanning and penetration testing have the IT systems for which the security needs to be assessed as a starting point.

However, both forms of testing do not necessarily take into account which business functions these systems support, which of these functions are really crucial for business continuity, what adversaries could be interested and why (e.g. money or data theft, espionage), and what hacking techniques might be employed.

Next to that, vulnerability assessments and pen-testing do not consider the physical component of testing. Sometimes, a successful cyber attack finds its origin in the accessibility for an outsider of a workplace, or in weaknesses in the physical security of a data centre. Furthermore, these tests do not assess the full scenario of a targeted attack against an entire entity (including the complete scope of its people, processes and technologies).

To provide an appropriate level of assurance that key financial services assets and systems are protected against technically competent, resourced and persistent adversary attacks, the level and sophistication of testing must be increased, and testers must be armed with up-to-date and specific threat intelligence.

[25] See FSB Lexicon (FSB, November 2018).

"Both vulnerability scanning and penetration testing have the IT systems for which the security needs to be assessed as a starting point."

2.0 In-Focus: The Different Forms of Testing

Threat Led Penetration Testing

Threat Led Penetration Testing (TLPT, or Intelligence-Led Red Team Testing) addresses this.

Entities with cyber maturity at the evolving level are supposed to perform only vulnerability assessments, penetration tests and scenario-based tests, while entities with - or aspiring for - an advancing or innovating maturity level are supposed to also undertake TLPT.

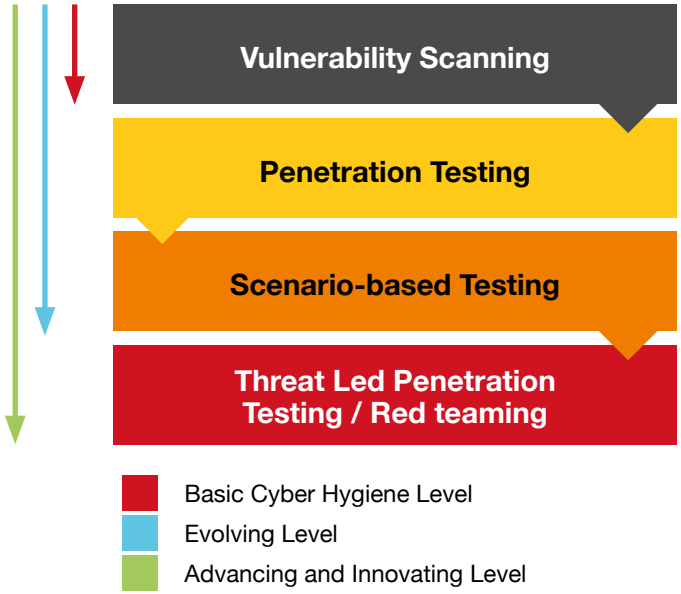


Figure 2: Testing vs cyber maturity

"While vulnerability assessments, penetration tests and scenario-based tests are useful in their own right and "must-do's" for any entity which relies on information systems for its activities, they do not mimic the real physical and online world in which an entity is active."

Threat Led Penetration Testing / Intelligence Led Penetration Testing

3.0 Threat Led Penetration Testing/ Intelligence Led Penetration Testing

3.1 Historical and Geographical Context of TLTP

Threat Led Penetration Testing (or Intelligence Led Red Team Testing) is a controlled attempt to compromise cyber resilience by simulating the behaviour (i.e. the tactics, techniques and procedures (TTPs)) of real-life threat actors, making use of ethical hackers (the so-called "red team").

It is based on targeted threat intelligence and involves simulating an attack on an entity's critical economic and business functions (CFs)[26] and underlying systems (people, processes and technologies), with minimal foreknowledge and impact on operations. Intelligence-led Red Team tests mimic the TTPs of advanced threat actors - whether malicious outsiders or an entity's own staff - who are assessed by threat intelligence as posing a genuine threat to an entity.

A TLPT also includes a level of "reconnaissance", i.e. the preparatory actions a threat actor undertakes to get a better insight into the entity's digital footprint, its people, processes and security controls. The test helps assess an organisation's protection, detection and response capabilities.

While vulnerability scanning and penetration testing focus on testing the cyber security of an entity's information and information systems, scenario-based testing and Threat Led Penetration Testing can be considered as cyber resilience testing, with TLPT being the most sophisticated form, especially suited for entities which play a key role in the financial system and/or real economy and have already reached a certain level of cyber resilience maturity. Authorities in several jurisdictions have set-up TLPT-frameworks and have urged their respective supervised entities (banks, FMIs etc.) to perform tests according to these frameworks.[27]

The first TLPT framework was developed in the UK by the Bank of England (CBEST, 2014),[28] followed by The Netherlands (De Nederlandsche Bank, 2016). The European financial sector is relatively well integrated, and some financial entities started to express concerns regarding the risk of proliferation of different TLPT frameworks.

Consequently, to ensure pan-European harmonisation in the development and roll-out of TLPT frameworks, the European Central Bank stepped in and developed the TIBER-EU framework (2018), which ensures maximum harmonisation, while still allowing for national specificities.[29]

"Authorities in several jurisdictions have set-up TLPT-frameworks and have urged their respective supervised entities (banks, FMIs etc.) to perform tests according to these frameworks."

[26] For identifying a financial entity's critical economic and business functions, most TLPT frameworks use the breakdown as developed by the FSB (Guidance on Identification of Critical Functions and Critical Shared Services / FSB, July 2013).

[27] See Guidance on cyber resilience for financial market infrastructures (CPMI/ IOSCO, June 2016, chapter 7).

[28] See CBEST Threat Intelligence-Led Assessments - January 2021 (bankofengland.co.uk).

[29] See What is TIBER-EU? (europa.eu). The TIBER-EU framework is entity agnostic and can be used outside the financial sector as well. It is also jurisdiction agnostic and can be implemented by authorities in non-EU countries.

3.0 Threat Led Penetration Testing/ Intelligence Led Penetration Testing

3.1 Historical and Geographical Context of TLTP

Currently, TIBER-EU is implemented in 13 European countries,[30] and more are expected to follow. The EU's Digital Operational Resilience Act (DORA) requires financial entities to establish a sound and comprehensive digital operational resilience testing programme as an integral part of their ICT risk management, including up to Threat Led Penetration Testing.[31]

Outside Europe, TLPT frameworks have been developed and implemented in Singapore (AASE),[32] Hong Kong (iCAST),[33] Australia (CORIE),[34] and Saudi Arabia (FEERT).[35]

These frameworks have been inspired by CBEST and TIBER-EU, and have benefited also from G7 guidance and work done by the Global Financial Markets Association.[36]

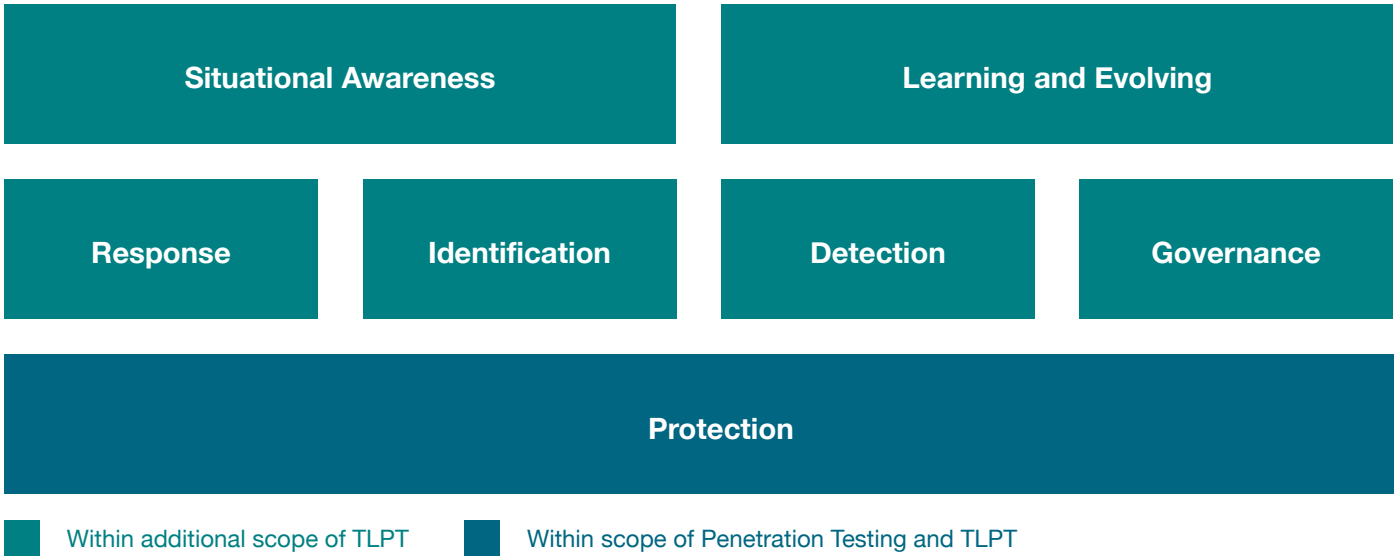


Figure 3: Illustration of additional scope of TLPT compared to traditional penetration testing (source: modified from HMA's C-RAF)

[30] Belgium, Denmark, Finland, Germany, Ireland, Italy, Norway, Portugal, Romania, Spain, Luxembourg, Sweden and The Netherlands, as well as the European Central Bank in its oversight capacity (status August 2022).

[31] DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT-related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogeneous across all EU member states. The core aim is to prevent and mitigate cyber threats··

[32] "Red Team: Adversarial Attack Simulation Exercise" (The Association of Banks in Singapore ABS, November 2018).

[33] "iCast - intelligence-Led Cyber Attack Simulation Testing" (Cyber Resilience Assessment Framework (C-RAF, Chapter 4), HKMA, November 2020).

[34] "CORIE - Cyber Operational Resilience Intelligence-led Exercises" (Council of Financial Regulators, July 2020).

[35] "FEERT - Financial Entities Ethical Red-Teaming" (Saudi Arabian Monetary Authority, May 2019).

[36] See G7 Fundamental Elements for Threat-Led Penetration Testing (G7, October 2018), and A Framework for Threat-Led Penetration Testing in the Financial Services Industry (version 2 / GFMA, December 2020).

3.0 Threat Led Penetration Testing/ Intelligence Led Penetration Testing

3.2 Common Elements of TLPT Frameworks

What all the TLPT frameworks have in common is strengthening the cyber resilience of supervised and/or overseen entities against advanced cyber attackers, ensuring financial stability. A Threat Led Penetration Test is no compliance exercise, nor is it a "pass or fail" test.

At the heart of a TLPT is **collaboration** between entity, Threat Intelligence service provider, Red Team service provider and authority; **evidence** in the form of results of controlled real-life attacks; and **learning and improvement** by replay and remediation planning.

TLPTs are executed on **live production systems** and are **intelligence-led** to emulate advanced attackers. In most cases, authorities closely follow the TLPTs, performed under the responsibility of the tested entity by **external, independent third-party providers** (Threat Intelligence (TI) & Red Team (RT) providers).

To mimic a real-life attack, the entity's defensive teams and staff should have no knowledge of the test being prepared and/or executed. Secrecy - until the test is completed - is of utmost importance.

Using external third-party providers for Threat Intelligence and Red Teaming services is important, to ensure test quality and integrity.

TLPT tests are highly intrusive and often managers feel their reputation is at stake.

It cannot be repeated enough that a TLPT is not a pass or fail test, and the learning and evolving experience is one of its key objectives. There is a risk that making use of internal threat intelligence capacity and Red Teams results in less challenging threat intelligence and - consequently - in less far-reaching attack scenarios.

External TI and RT providers are specialists, with broad experience of other clients, in and outside the financial sector. This ensures the designed attack scenarios are not only scenarios which have been already played out by real attackers, but also new scenarios which could be expected to be deployed in the near future.

A TLPT harbours elements of risk for all parties, owing to the criticality of the target systems, the people and the processes involved in the tests. The possibility of causing a Denial-Of-Service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of data, highlights the need for active and robust risk management.

The entity is responsible for implementing appropriate controls, processes and procedures to ensure the test is carried out with sufficient assurances for all stakeholders that risks will be identified, analysed and mitigated according to best practices in risk management.

Obviously, this includes applying minimal quality requirements with regards to the external TI and RT providers.[37]

[37] See TIBER-EU FRAMEWORK - How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu) (Chapter 6 Risk Management / ECB, May 2018).

3.0 Threat Led Penetration Testing/ Intelligence Led Penetration Testing

3.3 The Different Phases in a Threat Led Penetration Test

A typical Threat Led Penetration Test has four phases.

Depending on the involvement of the respective authorities and the applicable TLPT framework, the TLPT process can start with a *Generic Threat Landscape* (GTL) phase.

The GTL phase involves generic assessment of the national financial sector threat landscape, outlining the specific roles of the entities (e.g. investment banks, commercial banks, payment systems, central counter-parties and exchanges, for example), identifying the relevant threat actors for the sector and the TTPs used in the attacks.

The GTL will link these threat actors and the TTPs to specific entities within the sector and can be used as a basis for later attack scenario development.

The GTL may be validated and reviewed by the relevant national intelligence agency if possible and updated on an ongoing basis as new threat actors and TTPs emerge and pose a risk to the respective financial sector.

During the **preparation phase**, engagement for the TLPT is formally launched.

The teams responsible for managing the test are established; the scope of the test is determined, approved and attested to by the entity's board, and validated by the relevant authorities; and the TI and RT providers are procured to carry out the test.

The **testing phase** includes threat intelligence and Red Teaming. During this phase, the procured TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, providing a bespoke threat assessment, setting out threat scenarios for the test and providing detailed reconnaissance information on the entity (such as its digital footprint, perimeter and the people, processes and technologies that could be exploited), on the basis of which the Red Team (RT) provider will start its work.

Here, the TI provider works closely with the RT provider. Work on the Targeted Threat Intelligence from the TI provider and active reconnaissance work by the RT provider overlap, with the GTL being used as input, if available.

> *"The GTL phase involves generic assessment of the national financial sector threat landscape..."*

3.0 Threat Led Penetration Testing/ Intelligence Led Penetration Testing

3.3 The Different Phases in a Threat Led Penetration Test

The TTI Report and findings from the active reconnaissance work will be used by the RT provider to develop specific attack scenarios and to execute an Intelligence-Led Red Team test on specified critical live production systems, people and processes that underpin the entity's critical functions.

During the **closure phase**, the RT provider drafts a Red Team Test Report, which should include details of the testing approach and findings and observations from the test. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The main stakeholders will now be aware of the test and should replay the executed scenarios and discuss the issues uncovered during the test.

The entity should take on board the findings and then agree a Remediation Plan in close consultation with the supervisor and/or overseer. Finally, the process of the test will be reviewed and discussed.

To develop and execute possible threat scenarios, TI and RT providers not only need to be experts in their respective fields, they also need to have the right collaborative mindset and willingness to work closely together - and with the entity - while preparing and executing the TLPT.

It's not the purpose of this paper to discuss the details of different TLPT frameworks in-depth. We recommend referring to the respective frameworks mentioned earlier in this chapter.

GENERIC THREAT LANDSCAPE PHASE	PREPARATION PHASE	TESTING PHASE	CLOSURE PHASE
	Engagement, Scoping & Procurement (4-8 weeks)	**Gathering Targeted Threat Intelligence** (6-8 weeks)	**Reporting and Remediation Planning** (2-4 weeks)
		Attack Execution / Red Teaming (12 weeks)	**Replay Attacks** (1 week)

Figure 4: Typical TLPT process from start to finish (timings indicate time span, not person-weeks, and can partly overlap in practice)

Threat Intelligence and Red Team Service Providers: Trust and Assurance

4.0 Threat Intelligence & Red Team Service Providers: Trust & Assurance

4.1 Threat Intelligence Service Providers

Threat Led Penetration Tests harbour elements of risk for all parties owing to the criticality of the target systems, the people and processes involved in the test. The possibility of causing a Denial-of-Service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of data highlights the need for active and robust risk management.[38]

One element of an active and robust risk management is the quality of the Threat Intelligence and Red Team service providers and their respective personnel. A careful selection process is crucial to the success of a TLPT and for the continuity of the entity.

This is easier said than done. The lack of barriers to forming a cyber security company, combined with mushrooming demand for cyber services, mean more and more start-ups have been formed recently. It can be difficult to ascertain the professionalism of such companies.

So, Threat Intelligence and Red Team service providers should be selected according to some guiding principles and criteria.

Firstly, there is the reputation, history and ethical conduct of the TI and RT provider. Have they successfully completed other TLPTs, are references available and do they understand the legal and ethical challenges which come with a TLPT?

Secondly, it is important that a TI or RT provider gives high priority to their own governance, security and risk management, and applies the same high standards to TLPT activities.

Thirdly, what about staff competence?[39] Even if a service provider is able "to tick all the boxes" with regards to the above-mentioned principles and criteria, if it lacks competent staff, it will not be able to provide the procured services at the required (high) quality level.

A financial entity - and its respective authority - can check service provider's reputation with ease by making enquiries among those which have already undergone a TLPT. But ascertaining ethical conduct, risk management and quality of staff, for example, is more challenging. CREST (The Council of Registered Ethical Security Testers) - as neutral, not for profit organisation - has stepped in this void and offers industry-recognised accreditation services for TI and RT service providers and certification services for their staff, the cyber security professionals.

[38] See TIBER-EU Framework (Chapter 6, Risk management for TIBER-EU tests).

[39] There are more criteria which define the choice for a TI or RT service provider. For a more complete overview, refer to, for example the TIBER-EU Framework Services Procurement Guidelines.

4.0 Threat Intelligence & Red Team Service Providers: Trust & Assurance

4.1 Threat Intelligence Service Providers

TI and RT service providers can obtain company accreditation by CREST if they are able to prove compliance in four areas:

- Company operating procedures and standards
- Personnel security and development
- Approach to testing and response, and
- Data security.

Individual staff can have their qualifications, experience and competencies certified by CREST, after having successfully passed an exam in their field of expertise, such as penetration testing, threat intelligence, incident response or security architecture. CREST does not provide any cyber security services itself, nor does it provide training to individuals.

By doing so, it has no conflict of interest and is not in competition with cyber security companies. From this neutral position, it builds trust in the digital world by raising professional standards and delivering measurable quality assurance for the global cyber security industry.[40]

By expressing the expectation that TI and RT service providers have CREST accreditation and cyber security professionals have CREST certification, a financial authority can contribute to a more mature market for cyber security services in its respective jurisdiction, benefiting all.

"Individual staff can have their qualifications, experience and competencies certified by CREST, after having successfully passed an exam in their field of expertise..."

[40] See for more information on CREST: www.crest-approved.org.

Considerations for Authorities

5.0

5.0 Considerations for Authorities

5.1 TLPT: Some Practical Considerations for Authorities

As indicated earlier, Threat Led Penetration Testing is especially suited for entities which play a key role in the financial system and/or real economy[41] and have already reached a certain level of cyber resilience maturity. This is not the whole story, however. Threat Led Penetration Testing is not only challenging for financial entities, but it also requires a certain level of cyber maturity from the authority in charge and of the cyber security service industry in the country or region.

Research shows that cyber security service provision is at relatively low maturity levels in several developing countries.[42]

If authorities pursue a policy to have financial entities tested according to the respective Threat Led Penetration Testing Frameworks, they have to consider the possible capacity and quality restrictions of local cyber security service providers and consider options to catalyse development of the market for cyber security services.

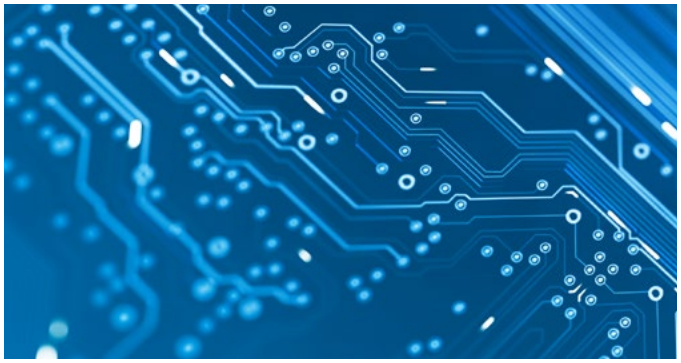
This includes an expectation that cyber security service providers and professionals meet objectively set minimum quality and conduct standards, (for example, as set by CREST).

Given these three restrictions (cyber mature organisations only, capacity limitations at the authority, and capacity and quality limitations in the cyber security services market), within a jurisdiction, the central bank and - if applicable - the supervisory authority need to agree on which entities should participate in any TLPT programme. The authorities need to decide whether a financial entity's participation in a TLPT programme is voluntary, or whether it is a supervisory obligation.

If there are authorities involved other than the central bank, it needs to be established which authority carries main responsibility for rolling out and executing the TLPT programme. Practice has shown in most cases this falls on the central bank.

Assuming the central bank is the authority in charge, it must invest in a dedicated team, headed by a senior manager, which must closely monitor each test process to ensure tests are performed according to the applicable testing framework and that Threat Intelligence and Red Team service providers meet the required quality criteria.

Ideally, to avoid supervisory judgement during the test process and the test becoming a mere compliance exercise, this team must sit at arms' length of the supervisory and oversight functions to ensure a smooth test process. As long as supervisors and overseers are involved in the scoping at the beginning and will receive the entity's remediation plan at the end of the test process, their responsibilities are well taken care of.



[41] Operational failure of such entities can negatively impact financial stability and could also include third-party critical service providers, especially if these third-party providers are part of the supply chain of several financial entities.

[42] See the outcome of the CMAGE study (Cyber security Maturity Assessment of the Global Ecosystem) as performed by CREST.

5.0 Considerations for Authorities

5.1 TLPT: Some Practical Considerations for Authorities

Such an approach could be challenging for a central bank with limited resources. Therefore, a central bank can make the deliberate choice being less involved in the daily monitoring of the test process, leaving it to the financial entity to ensure that a real independent and challenging Threat Intelligence Led Penetration Test is performed, without cutting corners.

Following this route, each central bank has to find for itself a balance between daily involvement in the test process and no involvement, keeping in mind also that lesser involvement could endanger the quality and credibility of the test - and therefore recognition of the test results by authorities from other jurisdictions.

This could possibly result in the need for the entity to duplicate tests. Also, no involvement in the test process could deprive authorities from extracting overarching, thematic findings from these tests, preventing shared learning.

Given the sensitive nature of Threat Led Penetration Testing, decisions on TLPT programme adoption, financial entity identification and responsibility should be taken by the authorities' board and communicated to the financial entity's board.

To smooth this process, a pilot test on a volunteering entity could be conducted first, setting an example for other entities to follow.

One thing all TLPT frameworks have in common is that responsibility for overall planning and management of testing lies with the entity being tested, not with the authorities. The entity must ensure all risk management controls are in place to facilitate a controlled test.

Once the decision has been made to set-up a TLPT programme, the authority must draft its own TLPT framework implementation guide. There is no need to invent the wheel again, as different Threat Led Penetration Testing frameworks have been developed and implemented by several authorities in Europe and Asia.

While these TLPT frameworks all have their similarities, they all differ in detail due to differences in financial sector set-up, in mandates of authorities, and in regulatory and legal differences. Therefore, while drafting a TLPT framework implementation guide, for a central bank, it is worth staying close to proven TLPT frameworks, but tailoring these to the unique needs of its own financial sector.[43]

"One thing all TLPT frameworks have in common is that responsibility for overall planning and management of testing lies with the entity being tested, not with the authorities."

[43] The TIBER-EU framework provides a good benchmark and can also be used freely by authorities outside the EU. While each implementation of TIBER-EU must ensure that all the core foundational concepts and approaches are adopted and implemented; each jurisdiction is free to adopt and implement further optional elements at its own discretion. Next to that, due to its comprehensiveness, the CBEST Implementation Guide is worth assessing (CBEST Threat Intelligence-Led Assessments - January 2021 (bankofengland.co.uk)).

5.0 Considerations for Authorities

5.1 TLPT: Some Practical Considerations for Authorities

Setting up and running a TLPT programme is a long-lasting endeavour for the authority and requires appropriate resources and management attention. Depending on the size of the financial sector, it will take time before all identified entities have gone through a Intelligence-Led Red Team test.

We know the tests themselves take time, but there are also capacity constraints at the authority and the limited number of service providers qualified to do these kinds of tests - which means not too many tests can take place at the same time.

As we have said, Threat Led Penetration Testing is about learning and evolving, and is not meant to be a one-off exercise. Regardless of the successful implementation of a remediation plan, the organisational and IT structure supporting an entity's critical functions, systems and assets is subject to constant change. At the same time, the capabilities of threat actors are further evolving. Testing at regular intervals is, therefore, a necessity.[44]

Finally, authorities pursuing a Threat Led Penetration Testing programme will help improve the cyber resilience of the most critical financial entities. Pursuing a TLPT programme will also contribute to maturation of the local market for cyber security services, benefiting other non-critical companies and society at large as well.

For the sake of common interest, achieving this objective requires close and constructive collaboration between all parties, private and public.

[44] As an indication, intervals of 3 years could be considered as appropriate.

From the Author

SecAlliance

With a background of more than 25 years in public service, Wiebe Ruttenberg joined SecAlliance as Director of Strategy, August 2021.

Prior to this he worked in senior policy roles at the European Central Bank (ECB), first as Head of the Market Integration Division (2006 – 2015) and finally as programme director focusing on technological innovation and cyber resilience across the financial sector (2016 – 2021).

In his latter position, he chaired the ESCB Task Force on Cyber Resilience Strategy for Financial Market Infrastructures, managed the Secretariat of the **Euro Cyber Resilience Board** and was member of the European Systemic Cyber Group of the European Systemic Risk Board.

The European cyber testing program **TIBER-EU** and the European Cyber Information and Intelligence Sharing Initiative **(CIISI-EU)** were developed and rolled-out are under his responsibility.

Before joining the ECB in 2006, he worked in senior roles at De Nederlandsche Bank and the Dutch Ministry of Finance."