NETITUDE

AN LRQA COMPANY

A comparison of Regulator driven Cyber Resiliency Frameworks and Approaches

A comparison between global financial services regulatory frameworks used for assessing operational cyber resiliency through threat intelligence led scenario based assurance testing. This review includes CBEST (UK), TIBER-EU (EU) and iCAST (Hong Kong).

AUTHORS: JEREMY GREEN, BEN DENSHAM, ANTHONY LONG

01 Contents

02 Executive Summary

2.1 'Houston, we have a problem…'

The operational resiliency of the financial services sector is of paramount concern to governments and regulators across the globe. A catalogue of high profile breaches suggests that board level engagement and awareness of how to prepare and respond to a cyber event is frequently misunderstood or inadequate. Although these boards believe that they are taking steps to combat the cyber threat, their strategies are frequently poorly grounded and misaligned.

As a consequence, the risk of a cyber-attack causing a significant impact to the operational stability of a financial institution, their customers and the wider supply chain is very real and is driving the advent of security testing frameworks.

To address this, a number of regulator-driven frameworks for assessing financial institutions cyber preparedness, protection, detection and response capabilities has matured, and proliferated across multiple regions around the globe.

Gaining assurance… …or not!

Financial institutions recognise that they are continually under attack and consequently have developed comprehensive assurance programs to measure their risks. However, it has been apparent that these assurance programs have often focused on the wrong assets, at the wrong time, and with the wrong vantage point. Assurance typically focused on internet facing assets, and less on the core banking platforms that underpin the financial institution.

In parallel, the activities were frequently point in time initiatives, focused on non-production assets, in a highly partitioned manner that addressed a highly defined scope. It was apparent that the assurance activities were not end-to-end, and did not mimic the Techniques, Tactics and Procedures (TTPs) of known real world threat actors.

In addition, typical assurance activities have an over emphasis on technical testing and are generally focused on measuring an organisations' defensive posture, as opposed to providing guidance on the robustness of an institution's detection and response capabilities.

Due to these shortcomings in assurance practices, it has been clear that some financial institutions have been much less prepared than either themselves, the regulator, or their clients would expect.

Operational resilience

Over the last four years, global regulators have shown increased interest in operational assessments, where they look to seek assurance and confidence in financial markets. This has resulted in the development of a range of regulator-driven frameworks developed in Europe and the Far East. The G7 Cyber Expert Group (CEG) has recognised that a global, collaborative, scalable approach is of great benefit. At the heart of regulators' concerns is the need and commitment to address operational resilience. Existing measures and rules are no longer enough, hence the introduction of operational resilience with a focus on enhancing cyber preparedness and response.

As regulator driven cyber resiliency frameworks develop and mature, it is essential for financial institutions to keep abreast of their cybersecurity responsibilities. In a world that is increasingly interconnected and global in nature, this could mean navigating regulatory frameworks across multiple regions and nations.

Regulatory response

In the same way that banks' financial resilience is subject to economic stress tests, Nettitude expect regulators to continue to stress test operational resilience, particularly where they disagree with organisations' self-assessments and internal testing and audits.

CBEST set the initial benchmark and introduced the new approach to validating organisations' cyber resiliency on real operational systems. TIBER-EU has matured this approach and scaled it up. With Far East regulators following suit and many other sectors developing similar standards, the value of threat led assurance testing has been clearly seen and is here to stay.

2.2 Context and purpose

Nettitude delivers comprehensive threat led assurance services that focus on the financial services industry and wider critical national infrastructure. Nettitude has built custom attack tooling, detection and response maturity models and regularly contributes to industry and academic research initiatives designed to mature this market segment.

From this experience and background, Nettitude has released this paper to provide an overview of cyber resiliency approaches taken by various regulators and financial authorities. This paper considers the differences between them, and provides guidance and recommendations on how to get the best out of them for your organisation.

It also looks to the maturity of threat intelligence led testing and how the approach should be matured and developed to meet the future demands of the threats faced.

This report is broken down into 4 main parts:

- **Section 3:** Background and objectives
- **Sections 4-7:** Overview, comparison and breakdown of the frameworks in detail
- **Section 8:** Recommendations and future developments
- **Section 9:** How should you respond?

03 Background and Objectives

3.1 Purpose of Threat Intel Led Testing Frameworks

Intelligence led assurance regimes are not new, and organisations are increasingly adopting threat led approaches to penetration testing. Benefits of this approach are:

1. **Advancing the boundaries** and value of conventional penetration testing by seeking to adopt the TTPs of **known threat actors** aggressively targeting organisations;
2. Seeking to address the concerns raised by regulators as to the actual cyber resilience of the **financial services sector**. Financial services organisations in turn needed to be reassured that the testing would be risk managed and controlled to reduce potential impacts to live operations.
3. Provides boards and senior executives with a **new level of understanding and clarity** as to the impact a cyber-event could have on their organisation. This also drives senior accountability and responsibility, conveying the importance of security to the board room.
4. Raises the **critical importance** of detect and response capabilities within organisations and moves people away from a reliance on defensive strategies alone.

One of the key wider outcomes that is characterised in all the emerging threat led simulation frameworks, and the way they are to be implemented, has been to guide the boards of financial firms, financial service providers and the interconnected supply chain into improving their resilience to real world cyber-attacks. They have created an appreciation of contagion risks that would otherwise be hidden or not understood.

CONTAGION RISK

Contagion risk is the risk that a shock to one financial institution spills over to others, or other markets/regions. In this way, small shocks can have significant effects. Contagion is one of the key dynamics that gives rise to systemic risk in a complex adaptive system.

3.2 Landscape Overview

The operational resilience of the financial services sector is paramount to maintaining confidence in the global banking system. Identifying cyber threats and security weaknesses that could affect individual firms or Financial Market Infrastructures (FMI) and their ability to respond is key to ensuring stability of the finance sector. Cyber resiliency is essential for firms/FMIs if they are to ensure the continued delivery of their products and services to the finance sector.

The UK finance regulators recognised the potential contagion impacts a cyber event could cause and the importance of cyber resilience. This drove the creation and launch of the CBEST framework in May 2014. The Bank of England **CBEST framework** is a threat-led approach to delivering assurance testing to regulated organisations within the UK financial sector.

Outside of the financial services sector, cyber resiliency has been central to the thinking of many other regulators within the UK. The **GBEST** scheme was piloted by the UK Government throughout 2017 and 2018, which was largely based on the approach taken within the financial sector. Similarly, **TBEST,** a scheme for the telecommunications sector, is based on CBEST and many other areas of the UK Critical National Infrastructure (CNI) are developing or implementing similar schemes (e.g. Aviation, Nuclear and Space). The UK **Civil Aviation Authority** (CAA) recently published CAP1574, a set of twenty-six security controls designed to be specifically applicable to cyber risks within the aviation industry.

The European Union (EU) implemented the Directive on Security of Network and Information Systems (NIS Directive) in August 2016 and this was subsequently adopted by EU member states, where the deadline for transposition of the directive was May 2018. The NIS Directive's purpose is to improve overall levels of information security and cyber resiliency for organisations deemed to be operators of essential services. The NIS Directive assigned competent authorities, bodies responsible for adapting the principals of the directive in their particular sector, such that operators of essential services can look to these entities for specific guidance.

The **European Central Bank** (ECB) released the European framework for **Threat Intelligence-based Ethical Red Teaming** (TIBER-EU) in May 2018 that was built on work by the **Dutch National Bank** (DNB) within their **TIBER-NL** framework. This is a much wider reaching programme designed not only for European financial services but also for other sectors. Seven European countries have now fully adopted TIBER-EU and launched their own versions.

Frameworks have also been developed in the Far East in **Hong Kong (iCAST)** and more recently in **Singapore** with the **AASE** (details and links provided in 'Table 1 - Intelligence led testing frameworks' on page 11).

Recognising that cyber threats are among the top risks to financial stability, the **G7 CEG** is seeking to address this and acknowledges that there is an increase in sophistication, frequency and persistence of cyber threats in the financial sector. It is essential to promote the consistency of cybersecurity approaches among G7 Partners – hence ensuring fundamental elements of threat led assurance frameworks are in place.

3.3 History of Assurance Testing Frameworks

Due to the continued widespread impact of cyber incidents and events, each producing significant disruptions, regulators have been shifting their attention from purely financial to operational resilience. Driven by rapid technological change, the continued impact of cyber attacks, a growing use of outsourcing, not to mention system outages, highlights the need to understand how a cyber event can have current and future knock on effects to business objectives.

This understanding has driven the need for more operationally focused, real world testing, in order to provide the right level of assurance to the regulators.

Within the UK financial sector, the use and impact of real-world testing scenarios against live systemically important operational systems understandably caused concerns, and as such, adoption of any testing against these systems has needed careful consideration. The UK Authorities, Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA) and the Bank of England (BoE), conducted a sector based exercise called Waking Shark in 2011, which was designed to simulate cyberattacks in order to test each financial institution's defences against real threats. There was a limited announcement by the BoE as to the outcome of tests, except to say that security is improving.

Traditional security programmes and penetration testing activities were being performed within these organisations, but limited scopes had in part resulted in the use of unrealistic testing scenarios that didn't highlight the actual weaknesses or vulnerabilities to critical functions overall, leading to a false sense of security.

This process did however highlight that even though significant money and resources were being put into cyber resilience programs, the result was not where it needed to be for the threats being faced.

The suggestions and recommendations made included "Increasing the stress on the sector in the cyber scenario, perhaps including more focus on the Advanced Persistent Threat (APT) strand", which could be seen as acknowledgment that a testing strategy more akin to real-word attacks should be developed.

3.3.1 UK Approach

In 2014, a more proactive stance was taken by the BoE and the Financial Conduct Authority (FCA), who asked CREST to develop a standard that could be used to test operational cyber resiliency within the systemically important financial infrastructure of the UK's financial system.

This brought into existence the STAR (Simulated Targeted Attack and Response) framework that then became the basis on which CBEST was built. The CBEST framework aimed to deliver regulator driven bespoke intelligence-led cybersecurity testing within the UK financial sector against live operational systems. The need to understand the real-world risks was essential and therefore a robust risk management process was built into CBEST from the outset.

3.3.2 European Developments

Within the EU a similar development took place initially in Holland from the Dutch National Bank (DNB) with the TIBER-NL scheme. This built further technical enhancements into the process and aligned the threat intelligence products more closely with the testing needs. The European National Bank (ECB) then developed the TIBER-EU framework that is designed to be a framework of frameworks for Europe wide adoption. Changes cater for the scale and complexity of a multi stakeholder environment with collaboration and cross border acceptance of testing results built in.

3.3.3 Far East Developments

In the Far East, Hong Kong developed their iCAST approach, which takes a more risk management starting point as opposed to a threat intelligence led approach. The latest framework is from Singapore with their AASE. The focus here is currently on the simulated testing phase.

The AASE is different to the other frameworks here in that is it written by a non-profit organisation that is providing guidelines for the financial industry in Singapore, as opposed to a regulator defining a framework to be followed.

3.3.4 G7 Statement

In October 2018 the G7 CEG issued a statement[1] on the next steps for strengthening international financial sector resilience. This built on a previous year's report (Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector[2]).

The statement included two documents that addressed fundamental elements for both 3rd party risk management and threat-led penetration testing. The latter aligns very closely with the CBEST and TIBER-EU frameworks in particular. It is clear that there is a need for individual Financial Market Infrastructure (FMI), sector and international levels to continue to develop recognised threat led frameworks that can effectively manage the cyber resiliency and assurance needs of multiple stakeholders.

3.3.5 Other Sectors

Outside of financial services, there has also been widespread interest from other sectors including the UK Civil Aviation Authority (CAA) with their developing of ATTEST[3], TBEST within the telecoms sector and the UK Government's GBEST programme.

1. https://www.fin.gc.ca/activty/G7/g7111018-eng.asp.
2 https://www.treasury.gov/press-center/press-releases/Documents/(PRA)_(BCV)_4728453_v_1_G7%20Fundamental%20Elements%20for%20Effective%20Assessment.pdf.
3 http://publicapps.caa.co.uk/docs/33/CAP1720ConDoc.pdf

3.3.6 Summary of History

The limitation from an assurance perspective of traditional penetration tests is that the targeting of critical systems is often narrowly defined, focusing on the technologies in order to reduce cost and risk. This approach to testing is inherently biased and does not take into consideration threat actors' real methods and techniques or the real attack surface presented by firms It also does not test the detection and response effectiveness in any meaningful way. Regulators needed a way to assess with a much higher level of assurance the real risks within the system, hence the creation of the intelligence led assurance frameworks.

Traditional penetration testing company accreditations and individual certification has been key to reassuring organisations that testing is conducted by adequately skilled individuals, is delivered by teams that understand how to manage the risks from offensive cyber simulations and will have limited impact on systems.

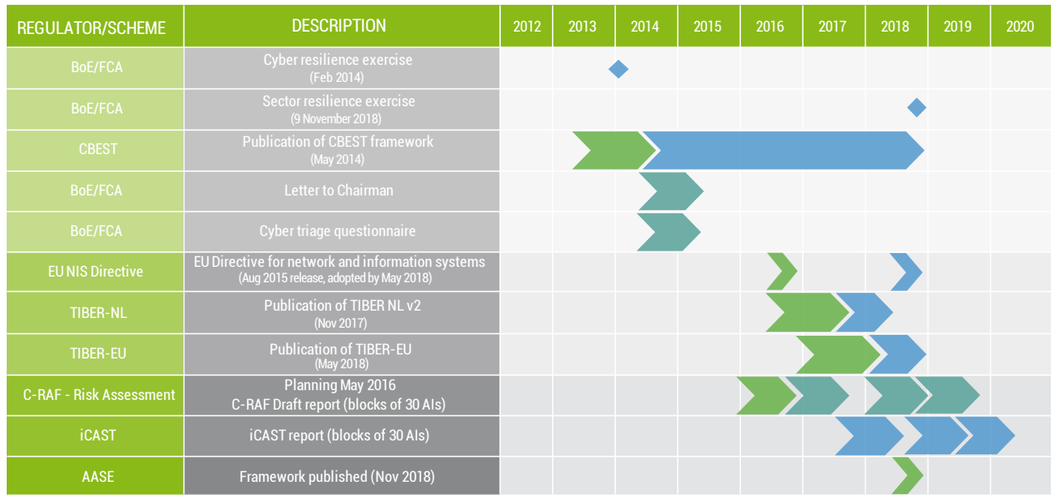


Figure 1 – Development time frame for attack simulation and intelligence led testing frameworks

04 Overview of Frameworks for Financial Services

Following the publication of CBEST, a number of further frameworks have been developed to support a similar approach for the Dutch National Bank (DNB), Hong Kong Monetary Authority (HKMA) and the European Central Bank (ECB).

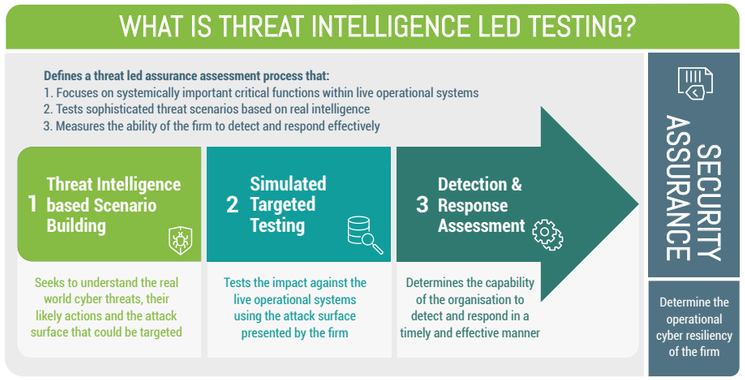
Framework	Regulatory Authority	Description	Published
CBEST[4]	Bank of England (UK) and Financial Conduct Authority (FCA)	Intelligence led testing framework	May 2014
C-RAF[5]	Hong Kong Monitory Authority (HKMA)	Cyber Risk Assessment Framework (C-RAF)[6] Intelligence Led Cyber Attack Simulation Testing (iCAST)	May 2016
TIBER-NL[7]	Dutch National Bank (DNB)	Threat Intelligence and Ethical Red Teaming -Dutch	Nov 2017
TIBER-EU[8]	European Central Bank (ECB)	Threat Intelligence and Ethical Red Teaming - Europe	May 2018
AASE[9]	The Association of Banks in Singapore	Adversarial Attack Simulation Exercise	Nov 2018

Table 1 - Intelligence led testing frameworks

4.1 CBEST

CBEST[10] is built on the CREST Simulated Targeted Attack and Response (STAR) methodology, which was created specifically to support the adoption of threat intelligence led, scenario-based assurance testing, ultimately across many sectors and regulated landscapes. CBEST is regulatory led where the scope of the Critical Functions (CFs) and Business Critical Functions (BCFs) to be included are agreed at the outset. A CBEST consists of three phases as follows:

1. **Threat intelligence** is conducted to identify and understand not only the most likely and most significant threat actor's capabilities, but also the threat surface as presented by the firm/FMI under test. A set of credible scenarios is created and supported by a targeting pack of information about the people, processes and technology that fall within the scoped threat surface. This work is conducted by an accredited external supplier and reviewed by the regulator and the UK Government's National Cybersecurity Centre (NCSC).
2. **An intelligence led penetration test** is then conducted for each of the selected scenarios where the TTPs deployed by the identified threat actors are enacted on the live operational systems. Testing on live operational systems was a key aspect of this approach set out by the BoE to ensure that all findings were based on reality.
3. **A Detection and Response Assessment (DRA)** is then conducted to assess the firm's/FMI's ability to detect and respond to the actions conducted during the test. A set of KPIs are measured around the firm's ability to conduct their own threat intelligence and the state of their detection and response.



CBEST is not a pass or fail exercise, but it produces a series of learnings and recommendations, which are to be presented back to boards and senior executives as well as the regulators. Post test follow-ups are then managed through normal regulatory interactions/channels.

Figure 2 – CBEST Process

4 https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity.
5 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180612e1.pdf.
6 https://www.cyberworld.com.hk/wp-content/uploads/custom/eDM/17Q3CW/CRAFreport.pdf.
7 https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp.
8 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.
9 https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf.
10 https://crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf

4.1.1 CBEST Core Objectives

The CBEST framework set out to achieve the objective of increasing the UK Financial Sector's resilience to cyber attack, but also support the following:

1. Access to advanced and detailed cyber **threat intelligence;**
2. Testing of **live systems;**
3. Access to **knowledgeable, skilled** and competent cyber threat intelligence analysts, who have a detailed understanding of the financial services sector;
4. Realistic penetration tests that **replicate sophisticated, current attacks** based on current and targeted cyber threat intelligence;
5. Access to highly qualified penetration testers that understand how to **conduct technically difficult testing activities,** whilst ensuring that no damage or risk is caused;
6. **Confidence** in the methodologies utilised by the companies within CBEST for conducting these sophisticated and sensitive tests;
7. Confidence that the results and the information accessed by the testers will be protected;
8. Standard key performance indicators that can be used to **assess the maturity** of the organisation's ability to detect and respond to cyber-attacks;
9. Access to **benchmark information**, through the key performance indicators, that can be utilised to assess other parts of the financial services industry; and
10. A framework that is underpinned by comprehensive, enforceable and meaningful **codes of conduct** administered by a specialist professional body.

4.2 TIBER-EU

As time has progressed, it has become apparent that intelligence led assurance programs have enhanced the resiliency of the financial system. Consequently, multiple regulators around the world started to explore creating their own frameworks. Recognising the challenge of having multiple competing frameworks, the European Central Bank decided to look at building a pan-European framework that could be leveraged across the whole of the Eurozone. This framework has been called TIBER-EU, and it is designed to provide commonality of approaches, yet flexibility for domestic regulators to implement their own discrete assurance activities.

This framework continues the refinements started by TIBER-NL and builds further on the fundamentals of the CBEST intelligence led penetration testing approach. There is significant alignment between TIBER-NL and TIBER-EU frameworks, the main differences equating to the national verses the European scope and oversight requirements. At this stage, TIBER-EU only references the need for certified and accredited service providers and does not define minimum requirements. Adoption by national and European authorities is gaining pace with Belgium, Demark, Germany, Ireland, Sweden, France and Italy using TIBER-EU to develop and implement their own domestically focused TIBER regimes.

4.2.1 TIBER-EU Core Objectives

The TIBER-EU framework is designed to be used not only across all the national boundaries within the EU but also within other sectors. On one level it provides a much wider breadth and increased flexibility, but it is designed to be taken by a large range of authorities and adapted to suit local needs.

The core objectives are shown below:

1. **Enhance the cyber resilience** of entities, and of the financial sector more generally;
2. **Standardise and harmonise** the way entities perform intelligence-led red team tests across the EU, while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities;
3. Provide **guidance to authorities** on how they might establish, implement and manage this form of testing at a national or European level;
4. Support **cross-border, cross-jurisdictional intelligence-led red team testing** for multinational entities;
5. Enable supervisory and/or oversight **equivalence discussions** where authorities seek to rely on each other's assessments carried out using TIBER-EU, thereby **reducing the regulatory burden** on entities and **fostering mutual recognition** of tests across the EU; and
6. Create the protocol for **cross-authority/cross-border collaboration**, result sharing and analysis.

4.3 C-RAF (iCAST)

The Hong Kong Monetary Authority (HKMA) has taken a slightly different approach through their Cyber Fortification Initiative, which has developed a Cyber Risk Assessment Framework (C-RAF) that includes elements of a maturity assessment and drives the scope of Authorising Institutions (AI) subject to Intelligence Led Cyber Attack Simulation Testing (iCAST) phases.

The Cyber Fortification Initiative has three pillars as follows:

1. **Cyber Resilience Assessment Framework (C-RAF)**

   This then has 3 core building blocks:

   a. **Inherent Risk Assessment** – Allowing AI to be classed as Low, Medium, High

   b. **Maturity Assessment** – AI determining whether the actual level of cyber resilience is commensurate with its inherent risk.

   c. **Intelligence Led Cyber Attack Simulation Testing (iCAST)** - Aimed at organisations that have inherent risk of medium or high.

2. **Professional Development Programme (PDP)**

   PDP acknowledges that certification is required but this relies on the support of the CREST programmes that have been developed for CBEST.

3. **The Cybersecurity Information Sharing Partnership (CiSP)**

   A sharing platform has been created for member entities to share intelligence and live information within the sector.

4.3.1 iCAST Core Objectives

Within C-RAF, the iCAST simulated testing does not have specific objectives defined, although the following purpose is set out:

- The **C-RAF** is a structured assessment framework for AIs to assess their inherent risks and the maturity levels of their cybersecurity measures against a set of principles set out in the **C-RAF,** called "control principles". Through this process, AIs will be able to better understand, assess, strengthen and continuously improve their cyber resilience.
- To facilitate this, the **HKMA** has introduced a new intelligence-led Cyber Attack Simulation Testing **(iCAST)** framework, which makes reference to the latest internationally recognised testing frameworks.
- Under **iCAST**, the traditional penetration test is augmented by further validation of the knowledge of the penetration tester(s) and introduces threat intelligence to formulate end-to-end testing scenarios. This will allow the tester(s) to more closely simulate real life attacks from competent adversaries.
- In addition, the **iCAST** provides **KPIs** that will help benchmark the ability of the AI to detect and respond to such attacks.
- **iCAST** is specially designed to, and preferred to be, run in the production environment to simulate a real-life attack, which also includes the assessment of the readiness of human and process elements of an AI.

4.4 AASE

The Association of Banks in Singapore (ABS) released a framework that defines the use of red team testing within Financial Institutions (FIs). It has also been written for use in other sectors and details the following:

1. An assessment of the organisational **resilience** against adversarial attack techniques, tactics and procedures.
2. **Identification of weaknesses** in security controls and associated risks not detected by standard vulnerability and security testing methodologies.
3. An assessment of the FI's **security incident management** and/or **crisis management** response and processes.
4. A safe, controlled opportunity to **identify and enhance the security posture** of a FI reducing risk of cyber compromise.
5. An opportunity for the defensive teams, such as the security monitoring or incident response team to **gain experience and be more proficient** in detecting and responding to incidents.
6. Provide **pragmatic direction** to the involved stakeholders as well as confidence in an informed post-activity short, medium and long-term security strategy.

05 Framework Comparison: Detailed Analysis Services

The table below provides an overview of the main characteristics of the four frameworks driven by regulators (CBEST, TIBER-EU and iCAST) and the red teaming approach put forward by ABS in Singapore.

	TESTING ATTRIBUTE	ASSURANCE RESILIENCY TESTING			
		CBEST	iCAST	TIBER-EU	AASE
	KEY FRAMEWORK ELEMENTS				
1	Threat intelligence	●	In some cases	●	N/A
2	Red team testing	●	●	●	●
3	Detect and respond assessment	●		●	N/A
4	Risk assessment of the organisation		●		
5	Maturity model mapped to industry standards		●		
6	Common scoring definitions for findings across all elements				
	CHARACTERISTICS				
1	Tests live operational systems	●	●	●	●
2	Regulator owned and developed framework	●	●	●	Industry body (ABS)
3	Exercise is supervisory led by regulators	●		●	
4	Clear guidance given around a white team/control group and governance	●		●	
5	Measurement of 'Detect & Respond' capability	●		●	
6	Proactively support cross border reporting and collaboration			●	
	OVERALL APPROACH				
1	Use of externally qualified organisations for threat intelligence	●		Not enforced	N/A
2	Use of externally qualified organisations for red team testing	●	●	Not enforced	
3	Use of externally qualified organisations for post testing response assessments	●			
4	Use of internal teams for threat intelligence			Collaboration	
5	Use of internal teams for red teaming				●
6	Findings and observations must map back to industry standards		●		
7	Uses MITRE ATT&CK framework				
8	Use of a standardised methodology	Build on CREST STAR	Own methodology	Own methodology	Own methodology
9	Use of individual certifications	CREST	CREST, and others	Various	Not defined
	REPORTING				
1	Use of national government agency reviews	●		●	
2	Target organisation measured for their own threat Intelligence capability (set KPIs)	●			N/A
3	Target organisation measured for their own detect & response capability (set KPIs)	●			
4	Formal reporting templates	●			●
5	Executive debriefs and management responses required				
	TECHNICAL APPROACH				
1	Real world simulation of threat actors/attack methods	●	●	●	●
2	Use of generic threat intelligence reports			●	N/A
3	Use of specific targeted threat intelligence reports	●	In some cases	●	N/A
4	Consideration of assisted footholds			●	
5	Creation of scenarios	TI Team	Red Team	TI Team	
6	Ability to update and add scenarios by Red Team			●	
7	Scenario 'X' based on opportunity and new tools/techniques			Considered	
8	Purple teaming option is provisioned			●	

Table 2 – Table overview of the frameworks

This is not a comprehensive list and does include some areas that none of the frameworks yet cover, but is designed to give a broad brush context to each of the approaches being taken.

This section now reviews the frameworks under a series of fourteen different headings.

5.1 Approach Taken

The approach to documenting the details of each framework varies considerably.
Table 2 (See section 6) details the phase and stage differences for the frameworks under review.

- The approach taken in **CBEST** is to define a number of phases and then provide concise details for a number of stages. The processes are easy to identify, and the output requirements can be determined for each stage.
- The **TIBER-EU** documentation aims to provide details in a number of ways, as diagrammatic process interactions, together with overview commentary.

  TIBER-EU is designed as a framework/s for the EU and this naturally introduces added complexity when trying to define the processes, as the information needs significant cross-referencing. Each central regulator in an EU country also has the remit to build on this framework for their own use.
- The **C-RAF's iCAST** component is based on CBEST. Details of the actual processes that need to be developed and followed are limited. The outputs from each phase are defined, but provide weaker expectations around the responsibilities of all stakeholders
- **AASE** is different to CBEST, TIBER-EU and iCAST in that it is designed to be guidelines for organisations conducting red team type activities. It is written by an industry body as opposed to a regulator themselves and is therefore aimed more widely than just as a regulator tool. AASE provides a strong focus on the simulated testing aspects, whilst keeping the threat intelligence and assessment of response optional and less defined. For example, the use of internal resources to deliver these aspects is welcomed – or may even be done as part of the testing engagement itself.

The following sections compare and contrast CBEST, TIBER-EU and iCAST. As AASE covers the red team phase in particular this has not been included as many of the wider components of the other frameworks do not appear within this.

This document aids in planning and executing such exercises but should not be relied on solely to achieve compliance with regulations.

5.2 Purpose and Objectives

CBEST was initiated in response to the need to assess the operational resiliency of the UK's financial services. CBEST provides direction on how to conduct a safe yet realistic simulated attack on the people, processes and technology that comprise of a firm's/FMI's cybersecurity controls. The aim is not only to test defences, but also the ability to detect and respond to a range of threats, including external attackers, insiders and those that could emanate from supply chains.

TIBER-EU is a framework of frameworks that delivers a controlled, bespoke, intelligence led red team test of entities' critical live production systems across multiple authorities. Designed to operate with multiple stakeholders and be adopted by relevant authorities on a voluntary basis. TIBER-EU is designed to be used as a financial stability tool or a catalyst to change. Relevant adopting authorities have the ability to define which entities could be tested and to add to the framework further as needed.

TIBER-EU is designed initially for core financial infrastructure (national and European) however other sectors and industries have been kept in sight. TIBER-EU allows for cross border testing with lead authorities, whose tests can be mutually recognised by other authorities, so long as the core requirements are satisfied.

TIBER-EU engagements are only recognised if conducted by independent third-party providers – they can't be completed or recognised through the use of organisations' own internal teams.

C-RAF is designed to strengthen the cyber resilience of financial organisations in Hong Kong, through a structured assessment framework looking at the inherent risks and maturity levels of their cybersecurity measures against a set of principles set out in the C-RAF, called "control principles". Through this process, AIs will be able to better understand, assess, strengthen and continuously improve their cyber resilience. iCAST is the threat led testing component, which compromises one part of the C-RAF.

5.3 Initiation and Initial Risk Assessment Phase

Regulators and authorities have used various methods to identify entities who must adopt their particular testing framework. All the regulators have determined that some level of risk assessment is required to prioritise the most at-risk firms/FMI providers/authorising Institutions' (AI) and entities.

The BoE, PRA and FCA have developed questionnaires to establish a risk score for the firms/FMIs, but these sit outside of the **CBEST** framework. Selection of firms/FMIs for testing is initiated by the regulators. Operational systems must be targeted, and no DDoS activities are expected to be included.

Within **TIBER-EU** there is no defined risk-based approach in place to determine which of the entities need to be included, the establishment of the framework and its scope are left to the authorities to determine. The scope from the ECB is passed to the local governing entities to manage.

An inherent risk and maturity assessment is a formal part of the **C-RAF** framework, and gives clearer guidance on how the assessments are to be conducted. Guidance in the appendix sections give granular breakdowns of the services, size and functions of the firms that align to help define risk ratings.

5.4 Scope

Within **CBEST**, all stages of the assessment phases are required, which provides a clearer definition of the processes to follow. Scope of the CFs/BCFs and the compromise actions that would cause the impacts to be tested are agreed with the regulator prior to any service provider being engaged.

More flexibility exists within **TIBER-EU.** Optional elements are defined within the framework, generally relating to the use of external parties such as intelligence agencies. Defined critical functions can be supplemented and the controls flagged, although agreed with the regulator, can be adapted based on feedback from the Threat Intelligence (TI) and Red Team (RT) provider's findings as the test progresses.

All stages of the **C-RAF** process are required, but the extent of the use of the threat intelligence report findings is based on risk. AIs that have a lower level of assessed risk can use a more generic threat intelligence report that is less tailored to their environment.

5.5 Process Overview

The CBEST framework highlights that the phases only represent a logical review of the tasks and there will be significant overlap. There is scope for activities to start earlier and run in parallel with others in order to increase efficiency, given the limited timescales of the assessment. The overall engagement timeframe between launch and supervision can vary considerably but is outlined as approximately twenty-two to thirty weeks.
Figure 3 presents a more realistic depiction of a physical project plan to complement the logical phases.

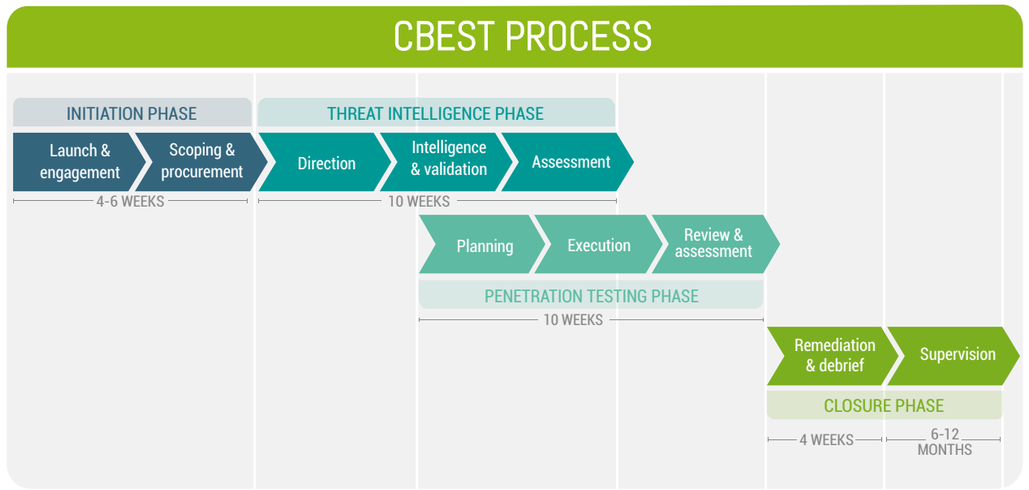


Figure 3 - CBEST Process

Although the overall process outlined in TIBER-EU is shown as relatively linear, within each phase there are additional details outlining the actual non-linear process interactions. The framework treats the TI and RT interactions as a single collaborative testing phase, which runs in parallel. It is envisaged that the overall process will take between twenty-three and twenty-seven weeks without TI/RT service provider procurement. The overall process is show in Figure 4.

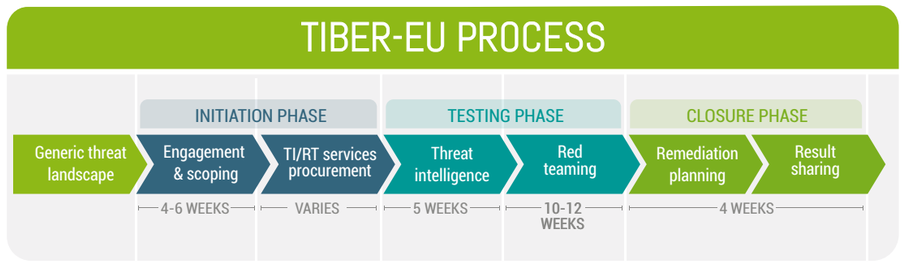


Figure 4 - TIBER-EU Process

A very linear process model is defined within the C-RAF framework, with each phase completing before the next one can start. The three stages of C-RAF are shown below:

1. Inherent risk assessment;
2. Maturity assessment (twenty-five components within seven domains); and
3. Intelligence-led cyber-attack simulation testing (iCAST).
   a. Scoping, developing threat intelligence analysis, developing testing scenarios, testing and reporting

There is no indication of envisaged timescales for the overall process. The overall process is shown in figure 5.

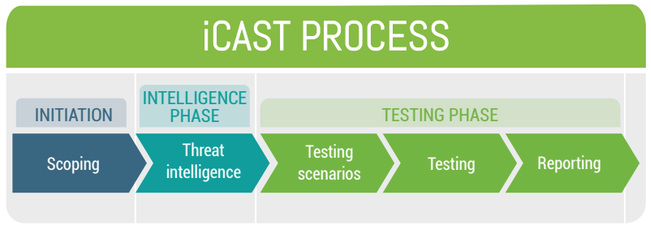


Figure 5 - iCAST Process

5.6 Testing Approach

Testing frameworks may allow an organisation to select different service providers for threat intelligence and penetration testing phases. Each framework takes a different approach to ensuring adequate communication and collaboration occurs between the two phases.

CBEST limits the interaction between the threat intelligence and penetration testing provider, by only focusing on the handover of assessment documentation to aid the penetration tester's planning. Collaboration and feedback are suggested as an aid to improving test success, but little further interaction is implied during execution. This defines a more rigid approach to reduce risk and ensure that tests are based on intelligence findings.

The **TIBER-EU** test phase sets out clearer guidelines on the interaction between the threat intelligence, the red team and white team, such that a more iterative approach is taken during the actual testing phase. It acknowledges that tests may not succeed and therefore an element of creativity can be employed. Robust management needs to be in place to ensure that exploiting further non-intelligence led scenarios is tracked effectively to reduce risk.

Specific handover between the threat intelligence phase and penetration testing phase is defined in **C-RAF,** with little further interaction during the testing phases. There are less details surrounding the interaction between the threat intelligence and penetration testing phases than the other frameworks.

5.7 Technical Phases and Capability

The frameworks break down the activity into two main areas, Threat intelligence and Testing. However, they all require some element of Security Operations Centre (SOC)/Incident Response (IR) assessment at the end, which is expected to be conducted by the testing provider as part of the testing phase.

This section covers:

1. Threat Intelligence Phase
2. Penetration Testing Phase
3. Detect & Response Assessment Phase

5.7.1 Threat Intelligence

CBEST requires threat intelligence management and targeting reports with a well defined and structured approach. The threat intelligence provider builds the scenarios within the management report and the intelligence gathered is very focused on the organisation in question.

TIBER-EU starts with the Generic Threat Landscape (GTL) phase. This involves a generic assessment of the national financial sector threat landscape looking at the relevant threat actors and their TTPs. The GTL can be reviewed by national intelligence agencies and is updated on an ongoing basis. The GTL phase is not mandated so this would allow for CBEST intelligence products to coexist and be recognised. The TI provider delivers a Targeted Threat Intelligence report (TTI). This defines threat scenarios and useful background information about the entity's attack surface.

TIBER-EU also provides guidance for firms to be open and forward in giving the provider access to information around a business and technical overview of each critical function, any current threat assessments or threat registers and any examples of recent attacks they have experienced.

If the organisation has an internal TI team in house, the external TI provider should liaise and gather relevant information that will enrich the TTI report.

iCAST also allows for generic Threat Intelligence to be used, but only for an organisation with a lower risk rating. Bespoke threat intelligence is used for organisations with a higher risk rating. The risk ratings are defined from the risk maturity phase.

5.7.2 Penetration Testing (Red Team, PT Team, Testing Provider)

CBEST testing is designed to follow the agreed scenarios closely. A test plan is built from the TI reports and a risk workshop held to ensure the operational risks are being recognised and managed effectively. The precise approach to this is left to the firm/FMI and service providers to agree. Testing sets out to achieve the compromise actions against the CFs/BCFs and the test plan will define partial and full success against these objectives.

The **TIBER-EU** Technical Threat Intelligence (TTI) report defines the testing scenarios. The TI Provider is also expected to contribute to the final Red Team test report. This is slightly different to what we have seen with CBEST and seeks to provide more collaboration. The Red Team is expected to execute the threat scenarios and 'expand' on them.

For example, TIBER-EU suggests that the RT may want to expand or adapt TTPs if it believes that is what an attacker would do. TIBER-EU defines clear requirements for defining the flags to be captured.

Testing providers are also encouraged to consider any possible anticipated leg ups and assisted footholds, which are discussed with the firm/FMI at the outset.

TIBER-EU also allows RT providers to develop other types of scenarios with more evolved TTPs. For example, this allows for more forward facing adaptive methods that may leverage research, expertise and other techniques beyond what the TI provider scenarios define.

iCAST testing teams create the scenarios, unlike CBEST and TIBER-EU where this is done by the TI team.

5.7.3 Detect and Response Assessment

CBEST defines and documents a detection and response assessment (DRA) at the end of the testing phase. A KPI document sets out key metrics and questions to be asked. This phase is crucial in determining the level of capability the firm has in terms of detection and response capabilities.

Within the **CBEST** framework the firm's/FMI's, own intelligence, detection, response and analysis capability are evaluated throughout and this information is used as part of the evaluation process and comparison exercise. This appears to be a key element within the framework.

There are no comparable capability assessments conducted under **TIBER-EU**, and a significantly different approach is taken when assessing the Blue Team (BT) as this is based on replay exercises with the RT.

Within **TIBER-EU** the RT report is forwarded to BT, where they subsequently generate a BT report, which is used in the replay workshop.

The goal of this workshop is for the firm/FMI to learn from the testing experience in collaboration with the RT provider. A recommended approach is that the BT and RT work together to conduct a Purple Teaming exercise to identify the expected response to the tested scenarios.

There is an optional Purple Teaming exercise that can also be conducted.

The **C-RAF** draws out this information much earlier in the process, before testing commences. This potentially focuses more heavily on maturity rather than the capability to respond to threat scenarios. There is little detail on how the response to the testing is measured or assessed.

5.8 Risk Reduction

Understanding and minimising risk during the execution of testing is crucial. Each framework approaches this in a different way.

A **CBEST** control group is required during testing such that incidents can be escalated to determine if they are a consequence of the penetration test. The firm/FMI are responsible for the tests and as such can pause the testing by communicating this to the penetration test managers. The regulator gives overall governance, but operational risks are to be managed by the firm/FMI. This will rely heavily on the capability of the control group.

TIBER-EU acknowledges that the exercise is a balance between accuracy and risk and makes specific references to a grey box approach and emphasis on simulation. The white team are in control of the test and are the only group from the entity that has knowledge of the test scope and timescales. It is important that the test proceeds in order to assess the response, and the risk management activities need to be in place to ensure the test is controlled.

Within **C-RAF** a control group is established so that incidents can be managed to determine if they relate to the **iCAST** simulation. In order to test the responses, the incident must be allowed to continue, although the communications need to be limited to internal parties.

5.9 Testing Validity

Threat intelligence is used to determine a series of testing scenarios, which are then executed during the penetration testing phase. The extent to which the scenarios must be followed varies between frameworks.

The **CBEST** approach looks to define a clear mapping between the intelligence reporting and the developed penetration tests. This "Golden Thread" is required, to ensure that only identified scenarios are tested and to reduce the risks of unintended consequences occurring.

There is more flexibility within **TIBER-EU** for the penetration testing provider to adjust tests during the exercise. There may potentially be some level of scope expansion as the exercises proceed, resulting in difficulties of mapping back to the intelligence lead approach. The results would require more detailed analysis to ensure that there was full coverage of the scenarios.

The approach set out in **C-RAF** is less clear, as the threat intelligence providers may be internal resources and simply hand over the threat intelligence report to the penetration testing provider to enact. The validity of the tests may be difficult to determine in this case.

5.10 Regulator Governance

For **CBEST**, the BoE Sector Cyber Team (SCT) manage much of the interaction between the parties regulator, firm/FMI, threat intelligence provider, penetration testing service provider, NCSC. It appears much of the SCT's proactive role is to manage and ensure regulatory risks are addressed and facilitate meetings to define scope, and discuss actions, progress and deliverables. During the initiation phases, there is significant interaction with NCSC.

Currently CBEST does not detail anything on cross border testing - but CBEST results could be accepted by other regulators in different jurisdictions.

The **TIBER-EU** Cyber Team (TCT) provides overall governance to ensure testing consistency, but management responsibility for testing is with the entity's white team leader. The TCT Test Team Manager (TTM) is a representative of the lead authority and is in direct contact with the white team throughout the entire test to ensure that the test is conducted in a consistent and uniform manner. In order to communicate key findings across the sector, the TCT liaises with the TCT TIBER-EU Knowledge Centre (TKC) such that information on common threats and vulnerabilities can be aggregated. The TCT do not provide an equivalent intelligence interface role with the European Union Agency for Network and Information Security (ENISA), national intelligence agency/national cybersecurity centre/high-tech crime unit.

The TCT can reject a test's validity for other jurisdictions if it believes that it has not been conducted properly. Participation of entities in TIBER–EU can be voluntary or mandatory as determined by the relevant authorities.

When entities are regulated by multiple authorities, a highly collaborative approach is advocated. Ideally, a lead authority will oversee the engagement and together consider the geographic location, legal structure, locations of underlying critical infrastructure and required oversight arrangements/supervisory teams.

Within **C-RAF** there is no indication if there is a governing entity. References are made to authorising Institutions (AIs) and HKMA, but no equivalent cyber team.

5.11 Test Management

Management of the end-to-end process is crucial in order to both minimise risk and maximise effectiveness. Again, the approach to this and the level of direction varies across frameworks.

Under **CBEST**, the firm/FMI have responsibility to manage the process, and much of the test management responsibility sits with the penetration testing service provider. A control group does need to be established but this is only for escalation of CBEST related incidents.

TIBER-EU defines clearer management actions throughout the test lifecycle for the authority, TCT and TTM, service providers and entity's White team (WT) and leader. The WT liaise closely with the procured TI/RT providers and the TCT throughout the lifecycle of the test, to confirm with the TTM that the test is undertaken in a uniform and controlled manner.

There are no defined management roles within **C-RAF** although this is implied in the professional development programme, and references CREST international as the certification body.

5.12 Service Provider's Accreditation & Certification

Ensuring that threat intelligence and penetration testing services are delivered by competent individuals and providers helps to deliver a risk managed, consistent and mature result.

CBEST can leverage a prescriptive approach to certification, requiring the involvement of UK government intelligence and UK certification backed roles. This leads to the engagement of experienced service providers, utilising trained and effective resources to ensure that risks associated with the test are mitigated.

At this stage, **TIBER-EU** only reference the potential need for certified and accredited service providers and doesn't define minimum requirements for individual roles.

There is a risk that without certified penetration testers, and with the increased flexibility of the testing process, undesirable or damaging consequences are introduced. However, it is recognised that the European market does not have the breadth of companies and individuals to mandate this at this stage.

The **C-RAF** Professional Development Program (PDP) acknowledges that certification is a key element but aims to be flexible and defines a set of equivalent qualifications, although the entry level is set relatively low. This could lead to undesirable testing outcomes resulting from poor tester capability.

5.13 Management Qualification

As well as ensuring that third parties delivering services are suitably qualified, organisations are required to demonstrate how they are providing capable resources to manage the testing.

There are no specific requirements set for the capability of the firm/FMI control group within **CBEST**, although this is somewhat mitigated by more active management by the SCT.

Likewise, the WT members or leaders within **TIBER-EU** are not required to demonstrate capability. As the control groups are key to providing internal direction, there may be an increased risk of ineffective evaluation of their impact. Roles and responsibilities are defined in more detail though.

Qualification requirements are set out in the PDP for the **C-RAF** assessment itself, but not for the test management.

5.14 Stakeholder Clarification

Stakeholders are formally defined in **CBEST**, along with mandatory certification requirements, a defined procurement process and the governing role of the regulators and the SCT. This has ensured there is 'close' adherence to the defined process.

Within **TIBER-EU** a more detailed list of stakeholders/actors is defined for each phase, as the collaborative approach requires additional controls, as significant responsibility lies with the WT leader to co-ordinate activities.

Within **C-RAF** there are very few stakeholders defined, the implications are that reliance is placed on the use of certified roles to manage the exercise.

06 Framework Breakdown: Table Comparison based on Assessment Phases

The table below compares the main elements from the three most established frameworks: CBEST, TIBER-EU and iCAST.

Sub-Phase	CBEST	TIBER-EU	C-RAF (iCAST)
A: Initiation Phase			
Launch	SCT initiates the process with the Regulator(s).	TCT controls the process with the participating entity.	No specific reference to role of HKMA and whether there is a cyber team managing the engagement process. Infers that independent, qualified personnel can be used but could be internal.
Engagement	Collaborative approach driven by the SCT, who manage the engagement with the Regulator(s) and the firm/FMI.	TCT controls the process with the participating entity.	No defined roles from the HKMA to manage the engagement.
B: Scoping Phase			
Procurement	A CBEST procurement guide has been published. Key objectives of the procurement phase are to ensure that the TI service provider is selected based on their ability to provide consistent, accurate and relevant information. The PT are selected on their testing calibre together with the quality and depth of their technical research and development (R&D) capability.	A full procurement guide[11] published in Aug 2018 has been provided that includes selection of the TI and RT providers as well as guidance around the role of authorities in this selection process. Procurement guidelines acknowledge that ultimately the accreditation and certification bodies in the EU will take over the responsibility.	Little or no guidance on the selection of service providers. The framework maturity guidelines infer that this could be a suitably qualified internal team.
C: Threat Intelligence Phase			
Direction	Threat intelligence reflects a 'grey box' testing approach in contrast with the 'black box' approach used by penetration testers.	No specific corresponding phase.	No specific corresponding phase.
Intelligence	The CBEST TI provider takes into account sector threat actors and capabilities, as well as the attack surface presented by the firm/FMI, to develop in depth scenarios. Reviews with the SCT and the NCSC are held. The development of the detailed threat intelligence report is based on targeting reports that ensures it is relevant to the firm/FMI.	TIBER-EU factors in the use of a generic threat landscape (GTL) report that applies to all entities within the sector as a basis for the TI report. The TI provider uses this in conjunction with a detailed threat attack surface assessment for the firm in scope to build the scenarios. TI and RT providers must work together in a collaborative, transparent and flexible manner. A TI provider must demonstrate willingness and the ability to work in this way, sharing its deliverables with its RT counterpart for review and comment.	The type of threat intelligence report is based on the risk assessment. For lower risk AIs a generic assessment can be used, whilst a more detailed report needs to be created for higher risk AIs.
Validation	A final review of the reports is conducted by NCSC, with a follow-up workshop with all parties. At this stage, the PT service provider has started planning based on the information provided by the TI service provider. This review stage allows all parties to revise the approach based on feedback from NCSC. Note: Whilst a collaborative approach is encouraged, the linear process has often meant this is challenging.	At this stage feedback to intelligence agencies is urged, with the TCT coordinating feedback to the TI/PT. Workshops are arranged by the TTM to review the reports. Note: As this approach is more collaborative this is less likely to result in significant revisions.	No specific corresponding phase.
Assessment	Internal assessments are conducted to review the threat intelligence capability of the firms/FMIs. This provides valuable information to the regulator and is assessed during the remediation phases to highlight skills and capability gaps.	No specific corresponding phase.	No specific corresponding phase.
D: Penetration Testing Phase			
Planning	Indicates that the PT service provider should be relatively engaged at this point as there has been oversight of the threat intelligence report and the targeting report.	Defines the requirement for specific handover between the TI and RT service providers.	Testing team creates the scenarios. Less guidance on the process for developing the testing scenarios and only infers that they should be based on the TI report.
Execution	Within the testing phase there is no formal interaction between the TI and PT. The execution phase does indicate that the firm/FMI may steer the engagement so that testing is effective given engagement time constraints.	In addition to the information provided by the entity, the role of the TI provider can be enhanced during the testing phase. For the test to succeed, the TI provider can provide ongoing threat intelligence to the RT provider during the test.	Testing is relatively isolated and requires only limited interaction with the working group. Assumes a clearly defined handoff between TI and the RT phases.
Review	A formal review workshop is conducted between the regulator, firms/FMIs and PT service provider to initiate remediation plans based on the findings.	No specific corresponding phase.	No specific corresponding phase.
Assessment	Internal assessments are conducted to review the detection and response capability of the firms/FMIs by the PT service provider. This provides valuable information to the regulator and is assessed during the remediation phases to highlight skills and capability gaps.	No specific corresponding phase.	No specific corresponding phase.
E: Closure phase			
Evaluation	The SCT prepare a consolidated report covering the firm's/FMI's intelligence, detection and response capabilities.	Specific RT and BT reports are generated as a result of the exercise. These form the basis for a replay workshop where the RT and BT discuss the issues and agree the remediation findings.	The AI produce a simulation test summary that covers the results of the test and ability to identify, detect and respond to the simulated attack.
Remediation	The Regulator and SCT review and provide feedback on the proposed remediation.	The lead authority reviews and accepts the entity's remediation report and attestations are issued by the Authority, TI and PT service providers to confirm compliance with the TIBER-EU framework.	No specific corresponding phase.
Debrief	A review of feedback on the CBEST process from all parties.	360-degree reporting is conducted to gather feedback on the TIBER-EU process.	No specific corresponding phase.
Supervision	The regulator monitors progress on the firm's/FMI's remediation activities.	The lead authority assigns responsibility to overseers and supervisors. The RT/TI providers and the board of organisation sign an attestation to confirm the exercise was done under remit of TIBER-EU to ensure the outputs can be mutually recognised.	No specific corresponding phase.

Table 3 - Phase alignment within the frameworks

11 https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

07 Framework Summary of Findings

This section summarises the current status of the frameworks discussed in this document, based on the observations made during this analysis

7.1 CBEST

Current Status: Managed (Mature) – In use and has undergone initial revisions.

1. Focuses on the use of procurement stages to ensure higher level of TI/PT maturity;
2. Certification backed TI/PT qualifications to ensure competence and reduce risk;
3. Relies on BoE SCT to coordinate activities, and maintain consistency;
4. Ensures substantiated linkage between the TI and PT phases;
5. Aims to reduce the risk of testing by adopting a more formal approach.

7.2 TIBER-EU

Current Status: Repeatable (Evolving) – The framework has been released and numerous countries are now using their own versions for testing.

1. Acknowledges that engagement of service providers will be less controlled and not fully formed;
2. More far reaching objectives and scope outside of just financial services;
3. No clear guidance on use of certification to ensure competence of the parties involved;
4. The white team effectively share the management responsibility with the TIBER cyber team;
5. Advocates the use of generic sector base threat intelligence analysis to form the bases of targeted reports to improve effectiveness;
6. Clearer indication of the stakeholders, which is necessary given the increased framework flexibility;
7. Better details defining the white team, but could go further to address the level of skill and expertise of the entity;
8. Allows and seeks to generate much more collaboration between both TI/RT providers and the authorities testing cross border entities;
9. Less prescriptive and more scalable, which may lead to increased risks because of an iterative and flexible testing approach.

7.3 C-RAF (iCast)

Current Status: Initial (Less mature) – Missing key elements, which are present in the other frameworks.

1. Focuses on AI maturity, rather than TI/PT entities;
2. Role of certification is more flexible and linked to CREST schemes, but has low entry point;
3. Role of HKMA not defined;
4. No formal assessment of risk when performing the simulations;
5. A lack of framework details may lead to ineffective testing.

7.4 AASE

Current Status: Initial (Recently released) – Large focus on simulated testing (red teaming).

1. Large focus on red team testing;
2. Optional elements around threat intelligence with viewpoints being provided from within the organisation, if chosen;
3. Well defined red team process and gives some elements of technical methodology, but is almost too prescriptive in places;
4. Defined reports structures (x8) set out that probably need to be reviewed once the scheme is used;
5. AASE is designed to be a set of guidelines to be referred to when conducting red team exercises, rather than a regulators framework to be followed.

08 Recommendations and Future Developments

8.1 10 Tactical Improvement Areas

The following are areas Nettitude believes can be evolved and matured to further enhance and ensure that threat intelligence led testing frameworks remain agile and dynamic.

1. Separation of the TI phase reporting to cover common and targeted reports. This will allow better use of resources and ensure more consistency between assessments.

a. Regulators to commission TI management reports that detail threat actors, capabilities and overview of the landscape for the sector/geographies in scope.
b. These would be valid for a period of time (potentially six months) and available to all entities going through a threat led assessment within that period.
c. The TI provider would conduct an in depth assessment of the firm's/FMI's attack surface (targeting pack) and build scenarios using all data available.

2. The TI and PT collaboration phase needs to be less prescriptive to allow better realism and collaboration throughout the whole engagement.

a. Ongoing collaboration between PT and TI providers should be planned and catered for.
b. Accommodate and manage the opportunities for an adaptive approach.
c. Ensure the TI provider is present and contributing to the final reports and debrief sessions.

3. The firm/FMI control group (known as the white team) should be more closely controlled to ensure the integrity of the assessment.

a. Documented and defined minimum experience/ capability requirements should be set.
b. Specific and defined stakeholder roles.
c. Signed NDA confirming rules of engagement and items that would require disclosure (for example, being involved in the Firm's/FMI's IR escalation process).

4. The outcome of the assessment of the intelligence, detection and response capability of the firm/FMI should tie back to a control framework such as IS27001 or NIST.

a. Shows all findings linked to potential remediation actions under agreed frameworks.
b. Align to frameworks commonly used by the sector.

5. Use of the MITRE ATT&CK[12] framework to standardise the use and reporting of the adopted techniques.

a. Define in the TI report which attack technique families are commonly used by the threat actor being simulated.
b. Report in the PT phase the attack techniques that were simulated and used.
c. Ensure that the SOC/IR teams are assessed against their ability to detect and respond to the referenced techniques.
d. Ensures accountability and a future road map to be built around expected capability within the firm's/FMI's detect and respond function.
e. Provide heat maps against MITRE ATT&CK showing the areas tested and outcomes.

6. Build in Scenario 'X' to allow for future innovative techniques, opportunist actions and bespoke developed techniques that may be constrained due to time or scenario text.

a. More useful for more mature firms/FMIs where some element of success by their SOC/IR teams is had.
b. Can be used to push the envelope once more is known and has been experienced from the scenarios.
c. Will facilitate testing which is truly end to end intelligence driven, allowing tester actions, once inside an organisation's boundary, to mirror real world threat actors.

7. Consider 'continuous' testing period over six to twelve months where opportunist attacks based on changes within the firm's/FMI's attack surface, issues from change control or unpatched vulnerabilities can be found.

a. Would allow bespoke development of zero days as well as looking for the right opportunity.
b. More realistic scenarios and results will be obtained, as current accepted falsities where testing is condensed into short time windows will be removed.

8. Consider the involvement and inclusion of supply chains in testing, to emulate more realistic attacks.

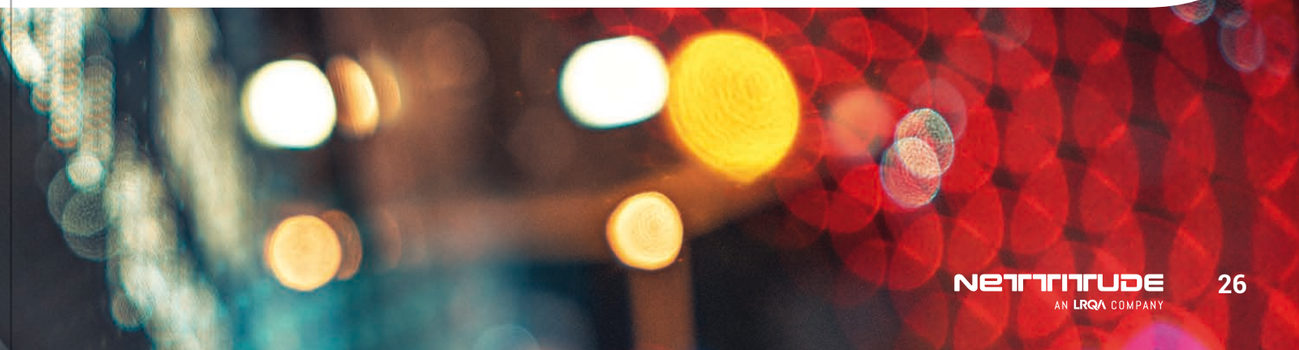
a. Would require more legal contract work to be in place between firms/FMIs and their third parties.
b. More realistic attack scenarios would allow supply chain risks to be taken into consideration and understood.

9. Split focus in reports and debriefs on pre-compromise and post-compromise actions.

a. Compromise will at some point happen. Ensure that any impacts seen from situations where assisted footholds are given carry the same weight as those that do not.
b. Considerable effort and time is often taken around the pre-compromise elements of scenario testing. The risk of entry by a real threat actor can never be fully eliminated so at one level entry to an organisation's network is inevitable with the right time and resources allowed. Time should be balanced in respect to this between pre and post compromise aspects of the scenario testing to ensure the full range of internal attack paths can be appropriately tested.
c. Consideration on how to best use and protect the IP and toolsets that RT providers have built up should also be recognised, although risks around this becoming widely detected is accepted to be with these providers.
d. Insider threats should always be included in tests, as post compromise actions can emulate insider actions to help better understand this normally overlooked threat.

10. Define the detect and respond assessment (DRA) as a distinct phase rather than include this as part of the testing phase.

a. Shows and aligns clearly the priority of the DRA assessment.
b. Ensure remediation actions are not just defensive, but include detection and response issues.
c. Build and use expected maturity models for DRA capabilities.
d. Consider a certified individual accreditation focused on detect and response capabilities. This person would work closely with the lead tester within the DRA phase to ensure a full picture and best practice remediation advice can be provided.



12 https://attack.mitre.org/

8.2 Maturity Model

Nettitude has developed a maturity model (Nettitude Maturity Model for Threat Led Testing (MM-TLT)) that demonstrates the differences between the current capabilities within simulated threat led testing frameworks and real attacks. This currently covers seven key elements, all of which can be flexed at different levels within individual tests. All of these capabilities could be simulated given the right level of focus, effort and time.

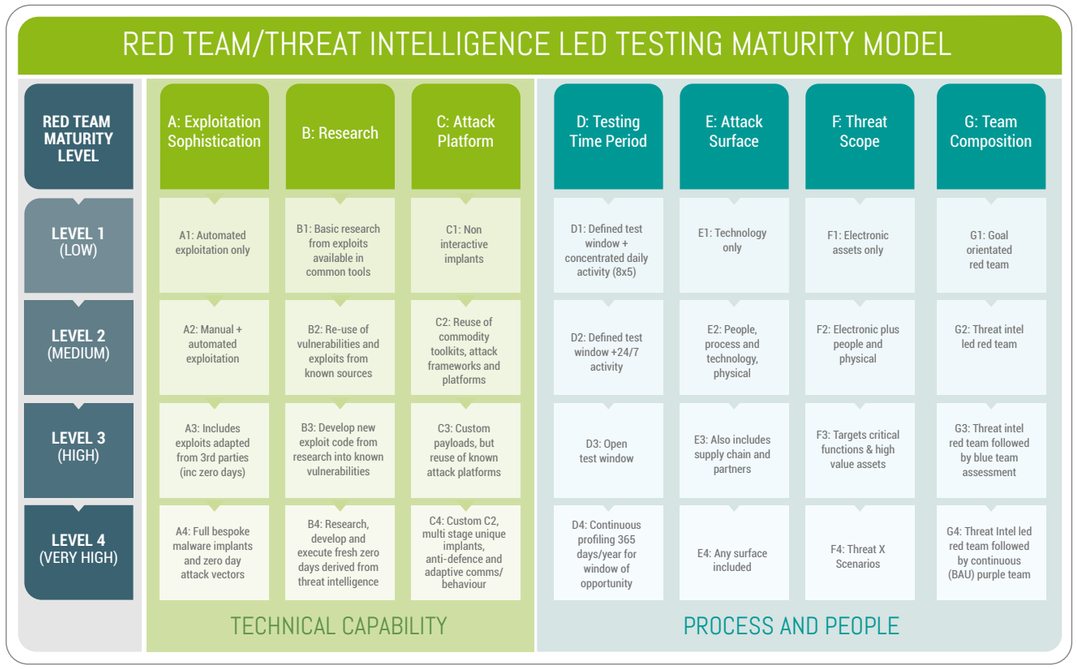


Figure 6 – Red team/threat intelligence led testing maturity model

- **A: Exploitation Sophistication**
  The ability to simulate attack complexity. The level of sophistication of the tooling used and the skills deployed in building, staging and executing exploit(s).
- **B: Research**
  The ability to research an attack surface, build tools and develop exploits/zero days for use within a given scenario.
- **C: Attack Platform**
  The ability to build and simulate attack infrastructure, communications and a simulated attack from start to finish.
- **D: Testing Time Period**
  The level of reality that can be simulated in relation to time scales. From limited daily hours through to waiting for the right opportunity.
- **E: Attack Surface**
  The level of restrictions and limits in place on the real attack surface available for use within a simulation.
- **F: Threat Scope**
  The breadth and variety of scenarios that can be simulated, including how they can be adapted based on the situation on the ground.
- **G: Approach**
  The level of completeness from attack testing through to detect and response assessments, to full purple teaming collaboration and learning.

8.2.1 Comparison with Threat Led Testing

The main areas where all the frameworks suffer currently is around the timescales to permit 'zero day' exploit development and opportunist elements to the attack scenarios.

With testing, there are always real differences compared to real world attacks due to legal, ethical and time constraints that will not be addressed by simulated attacks, but need to be recognised. These are acknowledged within the Singapore AASE. All testing activity must be:

1. Bound by law and ethics
2. Controlled by the target organisation, risk controls can be applied (i.e. Will not accept actions that are uncontrolled)
3. Respects the integrity and well-being of employees and partners (i.e. will not use physical/psychological violence and extensive coercion).

Threat led testing has had a significant impact on the financial resiliency of the financial sectors, where it has been used so far. Global adoption, recognition and alignment will be key as this continues to mature and develop further.

09 How should you respond?

Cyber risks have been traditionally hard for executives and organisations to understand due to the highly technical nature of the events and the obscure language used to describe and explain them.

Organisations that have been through threat led simulations and have experienced first-hand the likely impacts of a cyber attack are characterised by a step change in understanding, appreciation and realisation of the potential impacts.

Nettitude would encourage all organisations, financial or other, to support and embrace a threat led assurance process, as depicted in the emerging regulated standards, in particular:

1. Align your cybersecurity strategy with threat led frameworks. Understand and align your organisation with the latest thinking, approach and maturity to cyber resiliency. CBEST and TIBER-EU are leading the world in a robust assessment approach to cyber events.

No matter how much money has been spent, or how complex an organisation considers its cyber resilience and strategy to be, a threat led assessment will always validate and provide the reality on the ground about its effectiveness. Penetration testing has failed[13] at this, or to be fair, penetration testing was never designed for this purpose.

You should consider adopting a threat led assurance approach as a pillar within your own cybersecurity strategy regardless of any regulatory pressure.
By doing this you answer the questions:

a. What impact could a cyber event have on our organisation?
b. Would our organisation survive a targeted cyber attack?
c. Are the capabilities and operational functions in place effective in protecting the critical assets of our organisation?
d. Is our cyber strategy effective on the ground? If not, where does it fail and what are the priorities in addressing the exposures we have?

2. Liaise and work closely with regulators.
Cyber is a domain where sharing of information and keeping pace with the latest threats, mitigation approaches and sharing lessons learnt is essential and expected. Adopting a more collaborative approach with peers, regulators and the wider industry has already been shown to bring greater benefits. We all face a set of common threats, which have unique characteristics. Contributing from within our organisations, the experiences, challenges, skills and thinking that are effective will only be beneficial.

3. Expect to update, adapt and change your cybersecurity approach. Recognise that this is a fast paced changing landscape. Regulator assessments and cyber threats will continue to adapt, mature and change significantly. Your organisation's cyber strategy and approach will need to adapt in a similar manner.

13 This does not remove the need for penetration testing (it has a place and purpose), but it doesn't answer the same questions as threat led red teaming. Equally, threat led red teaming is not a substitute for traditional penetration testing.

10 Glossary

Term	Description
AI	Authorising Institutions
BoE	Bank of England
CAA CAP 1574	Civil Aviation Authority, CAP 1574[14], Twenty-six security controls for regulation
CBEST	Regulatory developed framework to deliver controlled, bespoke, intelligence-led cybersecurity tests
C-RAF (iCAST)	Hong Kong Monetary Authority Cyber Risk Assessment framework that includes elements of maturity assessment
CREST	CREST[15] is an international not-for-profit accreditation and certification body that represents and supports the technical information security market
ENISA	European Union Agency for Network and Information Security
FCA	Financial Conduct Authority (UK)
FMI	Financial Market Infrastructure
GBEST	UK Government testing framework, based on CBEST
GCHQ	Government Communications Headquarters, intelligence and security organisation responsible for providing signals intelligence and information assurance to the government and armed forces of the United Kingdom
Grey box	Approach to penetration testing whereby the tester has partial knowledge of the environment or organisation being tested
HKMA	Hong Kong Monetary Authority
NCSC	The National Cybersecurity Centre is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats. Based in London, it became operational in October 2016, and its parent organisation is GCHQ.
NIS Directive	The Directive[16] on security of network and information systems
Red team	A sophisticated approach to penetration testing. Red Team exercises often operate over an extended time and combine multi-faceted testing approaches that are designed to not only seek to penetrate an organisation but verify the response, monitoring and incident response investigation process and actions.
SCT	The BoE sector cyber team
STAR	Simulated Target Attack and Response
TBEST	Telecommunications testing framework, based on CBEST
TCT	TIBER Cyber Team
TIBER-EU	Published by the European Central Bank (ECB), a common framework that delivers a controlled, bespoke, intelligence led red team test of entities' critical live production systems
TIBER-NL	Threat Intelligence and Ethical Red Teaming developed by Dutch National Bank (DNB), and inspired by CBEST
TKC	TIBER-EU Knowledge Centre (TKC)
White team	Team of personnel, usually limited on a strict need-to-know basis, who have prior knowledge of an otherwise unannounced red teaming exercise

14. https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=8111
15. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
16. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com