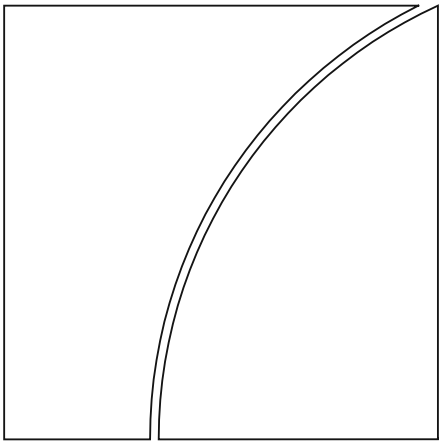
Financial Stability Institute

FSI Insights

on policy implementation

No 21



Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions

by Raymond Kleijmeer, Jermy Prenio and Jeffery Yong

November 2019

JEL classification: G18, M15

Keywords: cyber risk, cyber resilience, red teaming

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-306-3 (print)

ISSN 2552-249X (online)
ISBN 978-92-9259-305-6 (online)

Contents

Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions[1]

Executive summary

The cyber resilience[2] of financial institutions is one of the most critical concerns among financial sector authorities. As financial institutions become more digitalised and the sophistication of threat actors increases, financial institutions are becoming more exposed to cyber threats. Senior policymakers have warned that such threats could disrupt financial services and undermine security and confidence. From a supervisory perspective, consideration should be given to the potential of failure of a financial institution due to cyber weaknesses. Moreover, the possible contagion from such an event across the financial sector could give rise to systemic implications, and thus threaten financial stability.

Financial institutions and authorities are taking steps to strengthen the cyber resilience of firms. Financial institutions can use existing standards as a basis for strengthening their cyber resilience capabilities, and a range of testing activities to validate those capabilities. While each type of test has its intended objective, there is recognition of the importance of threat intelligence-led simulation of real-life cyber attacks through red team tests. Red team tests are useful to identify potential weaknesses in financial institutions' cyber protection, detection and response capabilities in order to establish an effective remediation plan.

This paper aims to facilitate deeper understanding by financial sector authorities on different existing approaches that authorities have pursued in establishing red team testing frameworks. The paper is based on information provided by eight financial authorities and selected private sector players. It describes key components of a red team testing framework, compares existing frameworks, outlines the benefits and challenges of such frameworks, and highlights potential cross-border issues relating to red team testing.

In general, a red team test can be divided into four phases: reconnaissance; getting into the institution; getting through its systems; and getting out with the captured "flags" as defined in the scenarios. Red teams can use either a methodology with a clear sequence of events in a cyber attack life cycle, or one that focuses on techniques from the different tactics deployed by threat actors and jumps from one point in the attack life cycle to another depending on the situation. In terms of scope, a red team test typically covers the entire financial institution involving different teams, potentially including external threat intelligence[3] and test providers.[4] The test is conducted without the knowledge of those responsible for protecting the institutions from cyber attacks.

Most of the surveyed jurisdictions have established red team testing frameworks with a number of common elements. The frameworks generally involve the following steps: defining the scope

[1] Jermy Prenio (jermy.prenio@bis.org) and Jeffery Yong (jeffery.yong@bis.org), Bank for International Settlements; Raymond Kleijmeer (r.kleijmeer@dnb.nl), the Netherlands Bank. The authors are grateful to contacts at the financial authorities covered in this paper and to Juan Carlos Crisanto, Matthew Hayduk, Rastko Vrbaski and David Whyte for helpful comments. Bettina Müller and Giada Tossi provided valuable administrative support with the paper.

[2] The Financial Stability Board Cyber Lexicon defines cyber resilience as the ability of an organisation to continue 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.

[3] Threat intelligence refers to information on cyber threats facing an industry or a specific institution (eg specific threat actors likely to target the institution and the likely tactics, techniques and procedures that they will utilise). In the red team testing context, such information may be provided by external private sector parties.

[4] These are private sector institutions whose service consists in providing the red teams with which to conduct red team tests.

and risk management controls for the test; procuring threat intelligence and red team providers; gathering threat intelligence; conducting the actual test; analysing the test outcomes; putting in place a remediation plan; and sharing the lessons learned with stakeholders.The frameworks apply typically to large or critical financial institutions, but authorities may have discretion to include other financial institutions. The frameworks, however, differ in terms of whether threat intelligence and red team test providers must be external to the financial institution, accredited and formally assessed.

An effective red team test is characterised by both firms and authorities being open about the results, learning from the weaknesses exposed and taking appropriate remedial actions. Unlike other risk assessment exercises, a successful red team test is not determined by whether a firm "passes" or "fails" the test. To truly benefit from red team testing, focusing on implementation of remediation measures after the test provides more value than just focusing on the test outcomes as evidence of weaknesses in the institution's cyber practices.

In the red team testing frameworks covered, financial authorities have different levels of involvement in the tests. In some cases, authorities are more involved and typically manage the conduct of the tests (ie oversee and guide the process of the test from start to finish, but do not take over responsibility of the test from the institution being tested). In other cases, authorities are less involved and instead focus their cyber resources on supervisory activities such as assessing the adequacy of financial institutions' cyber resilience, including ensuring that remediation measures identified during the red team tests are implemented in practice.

Sound technical and business expertise on the part of those involved in red team tests within firms, external threat intelligence and test providers as well as authorities is particularly important to ensure high-quality tests. Some authorities require external providers to be accredited or qualified so as to define a baseline of requirements for testers. In certain jurisdictions, the authorities do not require formal accreditation or qualification for several reasons, particularly scarcity of technical experts. Such flexibility is warranted to allow expertise to be cultivated while enabling firms to carry out the tests.

Establishing proper controls is also necessary to ensure the quality of the tests and to mitigate the risks. To help achieve high-quality tests, the existing red team testing frameworks describe expectations on procedural arrangements that should be put in place for the tests. These include expectations in terms of the scoping of the test, the selection of threat intelligence and red team providers, the formation of different teams and outlining their responsibilities. These procedural arrangements help in establishing a trusted environment among the different parties involved in the red team testing. In addition, these arrangements also enhance proper controls to mitigate risks associated with red team tests (eg risks to production systems and to sensitive information).

From a cross-border perspective, certain authorities may be prepared to recognise red team testing conducted under another jurisdiction's framework if certain conditions are met. Moreover, coordinated cross-border red team testing by financial institutions may be necessary to avoid jurisdictional blindspots and minimise unnecessary duplication of efforts by firms and authorities. This is especially useful for financial institutions with centrally managed infrastructures operating in jurisdictions with compatible frameworks. However, technical, operational and legal challenges surrounding such exercises are not easy to overcome currently.

Going forward, financial authorites may wish to clarify how red team tests fit within their strategy to improve the cyber resilience of financial institutions. Given that red team testing approaches are still evolving, it is important that authorities continue to assess the effectiveness of their frameworks and use the lessons learned from each test to improve the overall cyber resilience of the financial sector.

Section 1 – Introduction

1. **In recent years, financial institutions have faced an evolving cyber threat landscape from a wide range of threat actors.** Financial institutions have always been attractive targets of cyber attacks because of the substantial financial assets they hold. Sophisticated cyber attacks, which used to be almost exclusively the domain of nation states, are now commonly executed by sophisticated criminal groups that may or may not have ties with nation states. These developments prompted the G20 Finance Ministers and central bank Governors to warn in 2017 that these attacks "could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability".[5] This highlights the importance for financial institutions of having a strong security foundation in place. For financial authorities to fulfil their mandate of contributing to financial stability, this implies an evolvement of approaches used to assess institutions' cyber resilience posture.

2. **International standards have prompted authorities and institutions to take measures to improve financial institutions' cyber resilience posture.** The publication of the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures (FMIs) in June 2016 was the first internationally agreed guidance on cyber resilience for the financial industry and has been pivotal in providing a coherent approach to improving cyber resilience in financial institutions. The guidance called for FMIs to establish a comprehensive cyber resilience framework that includes a testing programme to validate its effectiveness. Such a testing programme could employ various testing methodologies and practices. Authorities and financial institutions alike recognise the importance of testing the overall cyber resilience posture of a financial institution by simulating tactics, techniques and procedures of sophisticated cyber attackers gathered from threat intelligence.[6]

3. **Enhancing cyber resilience and validating its effectiveness through testing requires consideration of various interlinked factors.** What follows is a description of the interrelationships between cyber resilience, testing, red team testing, and facilitating conditions.

- Implementing a cyber resilience framework. Cyber resilience is defined as "the ability of an organisation to continue 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".[7] There are existing standards that financial institutions can use to put in place stronger fundamental security measures. Examples are the International Organization for Standardization (ISO) standards for information security, the Control Objectives for Information and Related Technology (COBIT) Framework and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- Testing. Cyber resilience testing activities include vulnerability assessments, scenario-based tests (such as tabletop exercises to evaluate a firm's disaster recovery and business continuity capabilities), penetration tests and red team tests. Each type of test has its own intended objective. Authorities in certain jurisdictions have established requirements and/or formulated expectations on financial institutions' testing activities. The requirements typically apply to certain financial institutions based on, for example, their size, systemic importance, cyber maturity level, or the level of risk and complexity of their services or systems.

5 G20 (2017).

6 See eg Crisanto and Prenio (2017).

7 FSB (2018).

- Red team testing. Red team testing is one of the testing activities that can be used to validate cyber resilience in practice. It is defined as "a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations".[8] Red team testing mostly focuses on protection, detection and response measures. The outcomes of these tests could inform scenarios for testing activities that cover the response and recovery dimensions (eg disaster recovery and business continuity testing). In recent years, a number of jurisdictions have established frameworks for red team testing, partly prompted by the G7's (2018) fundamental elements for ethical red teaming or threat-led penetration testing.
- Fostering facilitating conditions. A number of facilitating conditions need to be in place for red team testing to be effective and for successful implementation of remediation measures. These facilitating conditions include board and senior management buy-in, a supportive culture and the availability of appropriate resources. These conditions will not only facilitate the conduct of a red team test but will also contribute to successful implementation of remediation measures identified during the test.

4. **This paper focuses on red team testing frameworks in jurisdictions that are known to have such frameworks in place.** As stated above, there is a range of testing activities to validate an institution's cyber resilience capabilities, each with its own intended objective. At the same time, there is recognition of the importance of threat intelligence-led simulation of real-life cyber attacks through red team tests. A number of authorities therefore may be contemplating establishing red team testing frameworks for their financial institutions. The paper aims to help those authorities by providing useful information about differences in existing red team testing frameworks, and the benefits derived and challenges faced by authorities in jurisdictions that have already implemented their respective frameworks. In particular, the paper covers the red team testing frameworks for financial institutions in the European Union[9] (including the implementation of the EU framework in the Netherlands); Hong Kong SAR; Saudi Arabia; Singapore; and the United Kingdom.[10] Authorities from these jurisdictions responded to a questionnaire, which was supplemented by interviews. A small number of private sector experts on red team testing were also interviewed to ascertain their perspectives on the issue. The insights gained from the completed questionnaire and interviews form the basis of this paper. The structure of the paper is as follows: Section 2 explains red team testing and its building blocks; Section 3 provides an overview of the commonalities and differences of the red team testing frameworks in the jurisdictions covered; Section 4 discusses the benefits and challenges of red team testing; Section 5 outlines the potential cross-border issues of red team testing; and Section 6 concludes.

[8] G7 (2018).

[9] The TIBER-EU framework was published in 2018, and a number of jurisdictions have started implementing the framework on a voluntary basis; see Section 3 for details.

[10] While currently without red team testing frameworks, Argentina and Mexico were included with a view to understanding the cyber resilience testing requirements or expectations in a sample of jurisdictions in Latin America. Moreover, while the EU red team testing framework has been implemented in other EU jurisdictions, only the EU-wide framework and its implementation in the Netherlands are included. The former in order to provide an overview of the overarching framework applicable in the European Union, and the latter in order to provide an example of implementation at the national level. It should be noted that the EU framework has been adapted from the Netherlands framework, which was established earlier.

Section 2 – Red team testing building blocks

5. **The term "red team" has a long history in a military context, where it is used to refer to "a way to think outside the box and to be able to anticipate and model adversarial behaviour".**[11] More concretely, the UK Ministry of Defence (2013) defines a red team as "a team that is formed with the objective of subjecting an organisation's plans, programmes, ideas and assumptions to rigorous analysis and challenge. Red teaming is the work performed by the red team in identifying and assessing, *inter alia,* assumptions, alternative options, vulnerabilities, limitations and risks for that organisation". Red teaming, therefore, can help an end user to critically evaluate its plans, programmes or projects, thereby leading to improved decision-making.

6. **In a cyber context, red team testing subjects an institution's cyber infrastructure to a simulated and realistic adversarial attack to test its resilience.** Large, global financial institutions have already started to put in place red team testing measures regardless of whether it is mandated by authorities in their jurisdictions. At the same time, as mentioned above, authorities in several jurisdictions have already established red team testing requirements for financial institutions.

7. **There is an opportunity to clarify what constitutes a red team test because of the different terminologies used.** See, for example, Section 3 for the different names of red team testing frameworks in different jurisdictions. The G7 also refers to red team testing as "threat-led penetration testing".[12] In practice, red team tests are quite different from penetration testing. Penetration testing is a test on an institution's information systems and involves the institution's defensive team from the start. The focus is on identifying vulnerabilities of the system being tested in order to improve protection against cyber attacks. NIST defines penetration testing as "a test methodology in which assessors, using all available documentation (eg system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system".[13] In contrast, as mentioned above, red team tests attempt to compromise an institution's cyber resilience, without the foreknowledge of the institution's defensive team, by simulating real-life threat actors based on information from targeted threat intelligence. This means that an institution's people, processes and technology are potential channels of attack under a red team test, and the focus is on understanding and improving how an institution protects, detects and responds to real-life attacks rather than on identifying system vulnerabilities. Table 1 provides an overview of the main differences of the two types of testing.

[11] Brangetto et al (2015).

[12] This term is also adopted in FSB (2018).

[13] This definition is also adopted in FSB (2018).

Main differences between red team testing and penetration testing

An overview of key characteristics Table 1

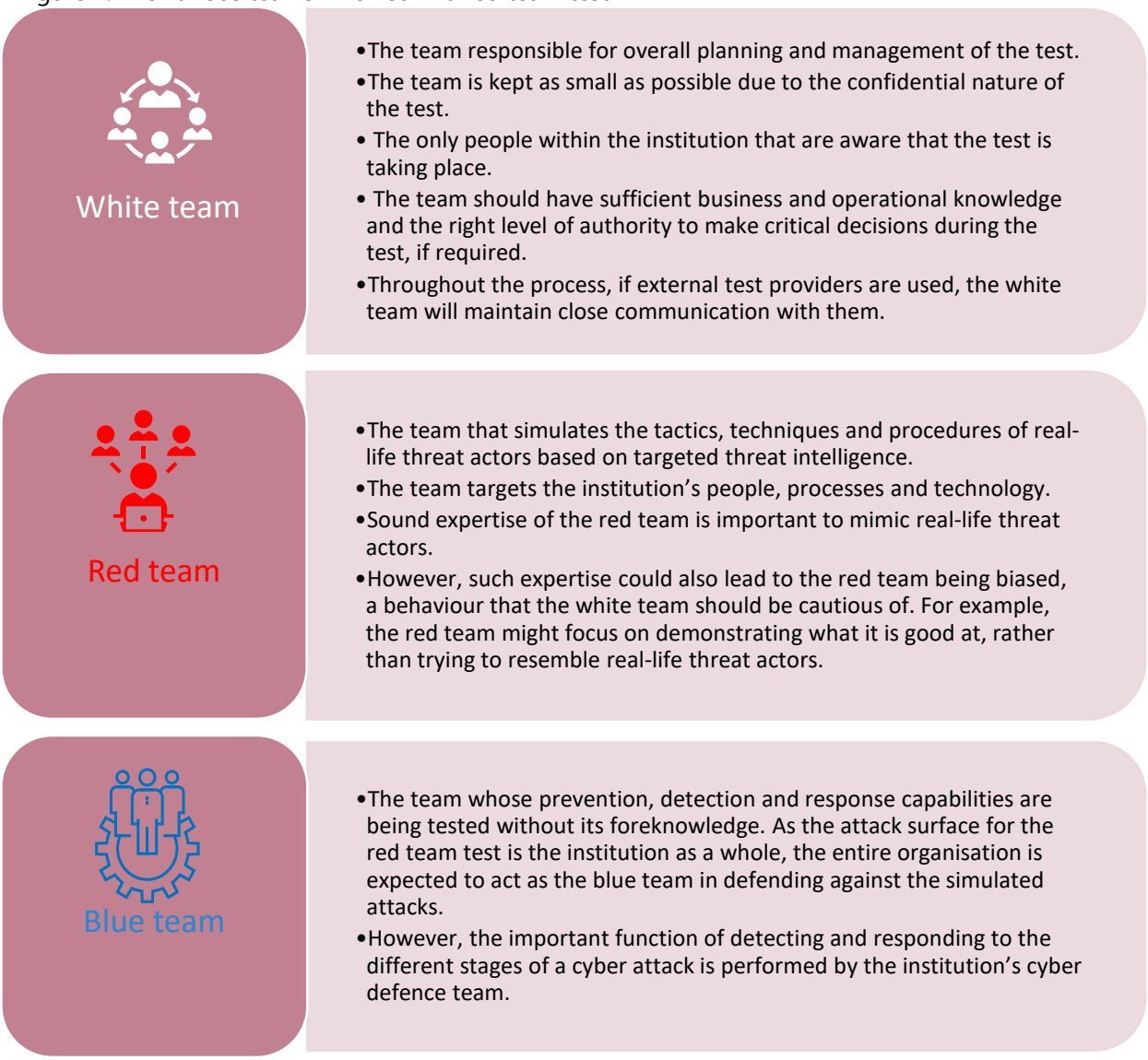
Characteristic	Red team testing	Penetration testing
Objective	To test resilience against realistic attacks in order to identify potential weaknesses in an institution's protection, detection and response capabilities	Gain insight into system vulnerabilities
Scope	Objective-based, open-scoped, designed to demonstrate critical impact to a business or organisation. Targets people, process and technology	Limited-scope technical assessment
Attack surface	Everything is "on"; scoped by white team*	Scoped by blue team
Defensive informed	Defensive team not informed beforehand	Defensive team informed and included in scoping of activities
Post-exploitation	Extensive focus on critical assets and functions	Very limited
Tested controls	Focus on protection, detection and response	Focus on protection
Test methods	Focus on realistic simulation; testing includes technical, human and physical factors	Focus on efficiency; testing includes mostly technical factors
Test techniques	Tactics, techniques and procedures (TTP)	Mapping, scanning and exploiting
Testing live systems	Live production systems	Typically limited interaction with live production systems
Duration	Months	Weeks

* See paragraph 8 for definitions of "white team" and "blue team".

Source: Saudi Arabian Monetary Authority (2019); Association of Banks in Singapore (2018).

8. **There are three teams within or outside a financial institution that are involved in red team testing, each with different roles.** These include the white team, the red team and the blue team. The white team plans and manages the test; the red team comprises the threat actors; and the blue team defends the institution from the red team attacks. These teams are organised for purposes of red team testing and are not necessarily standing organisational units within the institution. Moreover, the red team function of the test could be outsourced to an external party, or a combination of internal and external resources could be used. Figure 1 provides more details of the different teams and their respective roles.

Figure 1: The various teams involved in a red team test



9. **Effective procedural arrangements will need to be put in place to define the respective responsibilities of the different teams involved as well as the rules of engagement.** This includes establishing risk management guidelines and processes to address issues arising from the red team test as well as governance of the test within the institution being tested. Well defined procedural arrangements help in establishing a trusted environment among the different teams involved in the red team testing. A trusted environment, in turn, fosters more open sharing of the lessons learned from the test, which is one of its key objectives.

10. **A red team typically follows an execution methodology in performing the simulated attack.** In general, the actual testing is further divided into phases: reconnaissance; getting into the institution; getting through its systems; and getting out with the captured "flags" that have been defined in the scenarios. Red teams can use either a methodology that defines a clear sequence of events in the cyber attack life cycle,[14] or one that focuses on techniques from the different tactics deployed by threat actors and can jump from one point in the attack life cycle to another depending on the situation.[15] In

[14] See eg Lockheed Martin (2015).

[15] See eg MITRE (2017).

the red team testing frameworks covered in this paper, only one explicitly requires a specific execution methodology.

11. **Board and senior management buy-in is important to effectively conduct red team tests.** Board and senior management involvement sets the tone for the tests and how the test outcomes will be treated, addressed and used by the institution's management and staff. Hence, the board and senior management determines how supportive the institution's culture is of red team testing. Buy-in from board and senior management is also important to secure adequate resources to carry out the tests as well as to address deficiencies identified during the tests. Board and senior management buy-in also involves support for the neccesary controls and measures to be put in place to mitigate and respond to the risks of the red team tests (eg risks to production systems and to sensitive information). Some red team testing frameworks covered in this paper require active involvement by the board – for example, in the white team and more importantly in the remediation after a test.

12. **A culture that is supportive of red team testing contributes to its effectiveness.** In particular, a firm-wide culture that is more open to opportunities for learning would be more conducive to red team tests and could contribute more to improving the cyber resilience of the firm. For example, the board and senior management should regard weaknesses discovered by the red team as lessons that need to be learned and addressed rather than mistakes. Otherwise, a culture that focuses more on "mistakes" or "errors" would prevent realisation of the full benefits of red team testing and could leave the institution in a more vulnerable state. For red team tests that are required by authorities, the same openness to learning by authorities would be beneficial as well. To truly benefit from red team testing, focusing on implementation of remediation measures after the test provides more value than just focusing on the test outcomes as evidence of weaknesses in the institution's cyber practices.

13. **Appropriate resources, in the form of professional skills and qualifications, are an important factor in the successful execution of a red team test.** Within a financial institution, appropriate skills are needed to manage the whole test (white team) and defend against the simulated attacks (blue team). If the red team is comprised of external test providers, they will also need to be technically competent and qualified. In cases where red team tests are required by authorities, the authorities also need to have appropriate skills to properly oversee the tests, interpret the results and prescribe appropriate remediation plans. Existing red team testing frameworks put particular emphasis on the skills of red team testers. In general, red team testers are expected to:

- possess a minimum level of expertise – measured, for example, by certification criteria established by industry bodies;
- gain qualification through vetted industry examination processes; and
- be guided by a strict code of conduct.

Section 3 – Red team testing frameworks in different jurisdictions

14. **Several jurisdictions have put in place red team testing frameworks.** The European Union has its Threat Intelligence-Based Ethical Red Teaming framework (TIBER-EU), which is based on the previously developed framework in the Netherlands (TIBER-NL) and the CBEST framework in the United Kingdom.[16] Hong Kong has Intelligence-led Cyber Attack Simulation Testing (iCAST), Saudi Arabia has Financial Entities Ethical Red-Teaming (FEER) and Singapore has Adversarial Attack Simulation Exercises (AASE). CBEST has been in place for a few years now, while FEER is the newest, having been introduced in

[16] It should be noted that while TIBER-EU provides the red teaming framework for the European Union, implementation is left to the relevant national or European authorities. So far, apart from the Netherlands, TIBER-EU has been adopted in Belgium, Denmark, Germany, Ireland and Sweden, and by the ECB for purposes of financial market infrastructure oversight.

May 2019. The existence of official red team testing frameworks does not preclude financial institutions in these jurisdictions from conducting their own red team tests. Such tests are not subject to the requirements of the relevant framework. For example, in the United Kingdom, a commercial version of the CBEST framework called Simulated Targeted Attack and Response (STAR) can be used by financial institutions without the involvement of authorities.

15. **In most cases, financial authorities took the lead in developing the frameworks.** However, in Singapore, the Monetary Authority of Singapore partnered with the Association of Banks in Singapore to co-develop the AASE industry guidance. In the Netherlands, the development of the TIBER-NL was a joint partnership between the public and private sectors. Table 2 provides some key information about these frameworks.

Key information on red team testing frameworks Table 2

Jurisdiction	Framework	Year launched	Institutions covered	Threat intelligence and red team test providers		
				External parties?	Accreditation required?	Separate teams?
European Union	Threat Intelligence-Based Ethical Red Teaming (TIBER-EU)	2018	At the discretion of relevant national or European authorities	Yes	No	Yes
Hong Kong SAR	Intelligence-led Cyber Attack Simulation Testing (iCAST)	2016	Banks that aim to attain "intermediate" or "advanced" maturity level are required; banks with "high" or "medium" inherent risk are expected	Not necessarily	No	Not necessarily
Netherlands	TIBER-NL	2016	Institutions that are part of the core financial infrastructure, plus larger insurance and pension fund providers	Yes	No	Yes
Saudi Arabia	Financial Entities Ethical Red-Teaming (FEER)	2019	All regulated financial institutions are encouraged but, as a minimum, domestic systemically important institutions are required	Yes	Yes	No
Singapore	Adversarial Attack Simulation Exercises (AASE)	2018	All financial institutions are encouraged but larger ones are expected	Not necessarily	No, but encouraged	Not necessarily
United Kingdom	CBEST	2014	Critical financial institutions are expected; non-critical ones may opt in	Yes	Yes	Yes

Source: Published frameworks of the different jurisdictions and interviews with authorities.

16. **The red team testing frameworks have a number of common elements.** All the frameworks involve the following steps in the testing phases: (i) defining the scope and controls; (ii) procuring test providers; (iii) gathering threat intelligence; (iv) conducting the test; (v) analysing the outcome and establishing a remediation plan, where necessary; and (vi) sharing the lessons learned more broadly (see

Figure 2). In a way, this is not surprising since these are basically the same fundamental elements for threat-led penetration testing endorsed by the G7. The G7 fundamental elements, in turn, have been informed by the TIBER and CBEST frameworks, and together they have served as a kind of blueprint for red team testing frameworks for financial institutions around the world.

Figure 2: Common steps in red team testing frameworks

17. **The frameworks apply typically to large or critical financial institutions.** TIBER-NL and CBEST apply to critical financial institutions or those that are considered part of the core financial infrastructure in their respective jurisdictions. Large financial institutions are expected to undergo the AASE to complement their cyber resilience testing. iCAST, on the other hand, applies to financial institutions that are assessed to have "high" or "medium" inherent risk or those that aim to attain "intermediate" or "advanced" cyber resilience maturity levels. In some cases, financial institutions that are not covered in the frameworks are encouraged to, or can voluntarily undergo, a red team test. This is the case with FEER, which applies to domestic systemically important institutions at a minimum.

18. **Generally, the covered frameworks involve the same parties in the red team tests, although the level of involvement of the respective authorities differs.** A red team test generally involves the authority, the financial institution undertaking the test, and the threat intelligence and red team providers.[17] Some authorities are more involved than others in the tests. In such cases, authorities typically undertake a test management role (ie oversee and guide the process of the test from start to finish, but do not take over responsibility of the test from the institution being tested). FEER, for example, provides that the Saudi Arabian Monetary Authority's "green team" plays this role, while with TIBER-EU each authority has its TIBER Cyber Team (TCT). Red team tests, however, are quite resource-intensive. So, in other frameworks (eg AASE), authorities are less involved in conducting the tests but instead focus their

[17] See Section 2 for role of different parties involved in the test.

cyber resources on supervision activities. This includes assessing the adequacy of financial institutions' cyber resilience, including ensuring that remediation measures identified during the red team tests are implemented in practice. In terms of threat intelligence and red team providers, some frameworks provide that these be separate teams (regardless of whether from the same or separate companies). This addresses potential aforementioned red team biases. In addition to the parties mentioned above, in some jurisdictions there is also active involvement by the national security agencies. These agencies validate and/or contribute threat intelligence that informs the scenarios of the red team tests.

19. **All the frameworks covered have required controls that aim to ensure the quality of the tests and to mitigate the risks.** To help achieve high-quality tests, all frameworks describe expectations on procedural arrangements that should be put in place for the red team tests. These include expectations in terms of the scoping of the test, the selection of threat intelligence and red team providers, the formation of different teams and outlining their responsibilities. The procedural arrangements also enhance proper controls to mitigate risks associated with red team tests (eg risks to production systems and to sensitive information).

20. **Most frameworks also put emphasis on the qualification of the threat intelligence and red team providers as a means of ensuring the quality of the tests.** This explains the requirement in most frameworks for these providers to have accreditation or certification. Having the required accreditation is seen as indication that the provider has the requisite skills and competencies to either provide threat intelligence or conduct the test. In other cases, such as the TIBER-EU framework, the procurement of these providers is actively guided by authorities.[18] Financial institutions are also expected to conduct due diligence before procuring the services of external providers. Authorities interviewed also cite the important role of their own teams that coordinate and oversee the tests, as well as of the financial institutions' white teams, in ensuring the quality of the tests. Moreover, TIBER-EU requires that the firm, the threat intelligence and red team providers, and the lead authority furnish attestations confirming that the test has been conducted in accordance with the core requirements of the framework. However, there is recognition that whatever controls or structure are put in place, the quality of the tests will lack absolute consistency given that each test is different and could pose different challenges.

21. **In general, threat intelligence and red team providers are required to be accredited and external to the institution being tested.** For example, CBEST and FEER both require that threat intelligence and red team providers be accredited external parties. TIBER-EU (and consequently TIBER-NL and other EU jurisdictions and authorities adopting the framework) require these providers to be external to the financial institution being tested, but they need not be accredited. Accreditation is recognised as defining a baseline measure of the skill or qualification of the providers, but in itself does not guarantee the quality of the tests. AASE, meanwhile, takes a similar approach to accreditation. It encourages accreditation, but threat intelligence and red team providers do not have to be external parties. This approach recognises the limited pool of cyber skills in the jurisdiction, thus allowing flexibility for financial institutions to use their own resources as threat intelligence and red team providers. iCAST had a similar approach to AASE, but in June 2018 the accreditation requirement was relaxed.[19] Threat intelligence and red team providers no longer need to have accreditation as long as their expertise and experience are carefully assessed. The results of such assessments should also be properly documented.

22. **After a test has been executed, a review of the test is a formal part of the frameworks, and this review may include the assessment of the performance of threat intelligence and red team providers.** CBEST includes assessment of capabilities of the threat intelligence and red team providers as an explicit step and part of the reporting or documentation of the test. The TIBER-EU and TIBER-NL frameworks mention a "purple teaming" during which the red and the blue teams replay jointly the different phases of the test, and a "360° feedback" in which all the parties involved in the test provide

[18] For this purpose, the ECB published the TIBER-EU Procurement Guidelines in August 2018.

[19] HKMA (2018).

feedback on each other in order to facilitate the learning process as well as identify potential ways to improve future tests. A similar approach is followed by other frameworks such as FEER. However, some frameworks do not have explicit requirements for the authority to assess the capabilities of the threat intelligence and red team providers.

Section 4 – Benefits and challenges of red team testing

23. **Identification of potential weaknesses in financial institutions' cyber protection, detection and response capabilities is the main benefit of red team testing.** Red team tests are able to identify gaps and blind spots in financial institutions' cyber resilience practices. For example, one authority shared that red team testing is effective in identifying issues that are not picked up in cyber resilience maturity assessments. Red team tests can therefore flag any unresolved weaknesses and drive better understanding of a financial institution's level of resilience against current threats.

24. **Remediation plan to address identified weaknesses is required by all covered authorities.** Depending on the authorities involved in the tests, the responsibility to monitor implementation of the remediation plan could fall on supervisors (if financial stability authorities are involved) or the remediation plan is in itself seen as the ultimate output and is used to support supervisory activities. For example, in frameworks that involve supervisory authorities, the remediation plan can be used in determining the risk profile of financial institutions. In either case, while indicative deadlines may be set for the full implementation of the remediation plan, the timeline generally varies depending on the remediation measures or activities required. One authority mentioned that if significant weaknesses are identified during the test, the test would be paused in order to address such weaknesses.

25. **Strengthening a financial institution's cyber resilience posture is another benefit of red team testing cited by the authorities covered.** The main goal of red team testing is of course to enhance financial institutions' preparedness to address identified potential cyber threats through remediation plans. But the benefits of red team testing go beyond this. Testing should lead financial institutions to better organise threat intelligence and to develop realistic test scenarios that can be used for tabletop cyber exercises. It also fosters cooperation among different units within an institution, promotes strong security awareness and culture, and raises board and management accountability over cyber risk management. Red team testing therefore enables financial institutions to achieve an appropriate level of maturity in their cyber security controls and, hence, a stronger cyber resilience posture.

26. **Lessons learned from red team tests could potentially help enhance cyber resilience for the broader financial sector, but implementing this in practice is a challenge.** All of the red team testing frameworks covered provide for the sharing of key themes from individual tests, either among institutions that are required to undertake the test or with the broader financial sector community. These would include key findings, common threats and weaknesses, and common issues identified during the tests. This information is typically anonymised and aggregated, and disseminated through an established engagement channel. The information is useful in improving future tests and, more importantly, in enhancing the cyber resilience of the broader financial sector. However, most financial institutions may already find it challenging to fully address the issues they have identified, let alone issues identified in other institutions. Moreover, most authorities may understandably choose to focus on implementation of individual remediation plans instead of incorporating also lessons learned from other tests.

27. **Other benefits mentioned are those relating to authorities themselves.** Red team tests based on an established framework provide a baseline measure for authorities to evaluate the design and operational effectiveness of cybersecurity controls in financial institutions. Such tests therefore afford authorities a comparative view across financial institutions within their remit. In addition, through identification of common issues, weaknesses and capabilities, such tests provide a better understanding

of a sector-wide cyber resilience. This information is helpful in developing a forward-looking strategy on the part of authorities. Furthermore, as financial institutions realise the benefits of red team testing, they become more willing to engage with authorities on cyber risk. This, in turn, supports authorities' objective of enhancing overall cyber resilience in the financial sector.

28. **Getting participants to view red team tests with the right perspective is an important challenge.** Participants of a test could view it either as a "learn and improve" or "pass or fail" type of test. Financial institutions with a culture supportive of red team tests typically take the former view since their main goal is to identify and improve weaknesses in order to improve their cyber resilience. Authorities with more experience overseeing red team tests also typically take the former view. However, there is a risk that authorities (or even financial institutions) that may be new to red team tests may lean towards a more supervisory compliance or "pass or fail" perspective. This would be counterproductive and would reduce the effectiveness of red team testing as a tool to improve cyber resilience.

29. **The different perspectives taken by authorities may be illustrated in the pattern of their potential involvement throughout the different phases of the test.** Theoretically, less experienced authorities might tend to focus mostly on the actual test, perhaps because they devote more attention to spotting weaknesses or, more benignly, they might be concerned that something will go wrong with the institution's live systems during the test. More experienced authorities might tend to be more actively involved during the scoping and scenario design phases of the test, step back during the actual test when the testers take the helm, and get actively involved again during the closing and remediation phases.

30. **Most of the authorities covered highlighted challenges surrounding the limited supply of cyber expertise.** There may be limited cyber expertise within financial institutions, authorities, and threat intelligence and red team providers. Lack of competencies and capabilities may be particularly acute in smaller financial institutions. It could also lead to misalignment of expectations among the different parties involved in the tests. Hong Kong addressed this problem by explicitly incorporating the Professional Development Programme (PDP) in its Cybersecurity Fortification Initiative. The PDP involves a local certification scheme and training programme for cyber security professionals, which was developed jointly by the Hong Kong Monetary Authority, the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute. It aims to increase the supply of qualified cyber security professionals in Hong Kong.

31. **However, a few authorities do not expect limited cyber expertise to be a long-term problem.** A few authorities take a more optimistic view. They view shortage of skills, or of threat intelligence and red team providers in particular, as a short-term problem because they expect that a number of companies will eventually move towards providing such services if these are required by rules or regulations. They noted that this has been observed, for example, in the United Kingdom. In general, the financial industry in the UK has been able to attract skilled cyber security professionals due to relatively competitive compensation packages. The concern, though, is that this may be at the expense of other industries (eg telecommunications, energy), which could just as well expose the financial industry to vulnerabilities to the extent that there are interconnections. Another concern is that there could be concentration of cyber expertise in larger economies at the expense of smaller economies.

32. **Costs of conducting the tests also pose challenges.** Conducting red team tests can be costly to financial institutions. They may need to hire external threat intelligence and red team providers or acquire expertise in-house. This is on top of making sure that they have the right expertise to manage the tests and to defend against the simulated attack. The costs are particularly prohibitive for smaller financial institutions that may be required in some jurisdictions to undertake the test. Costs could also be challenging to authorities that also need to build expertise to oversee and manage the tests, to make appropriate use of the outcome of the test and to implement the necessary remediation measures.

33. **In a few jurisdictions, costs to authorities are partly offset by contributions from the private sector.** In the Netherlands, for example, participating financial institutions pay a third of the programme costs related to managing the test while the remainder is covered by the central bank. This is also the

approach taken in Belgium and Denmark, both of which have also adopted the TIBER-EU framework. This approach addresses part of the cost-related challenges and at the same time facilitates literal buy-in and commitment from financial institutions to the testing.

34. **Other challenges revolve around the actual conduct of the tests.** Practical challenges related to the tests include achieving a consistent level of quality of intelligence and tests provided by different external providers, establishing an environment that fosters trust among the different parties involved in the tests, and protecting the confidentiality of data that may be exposed to external parties undertaking the tests. Including third-party service providers (eg cloud service providers) in the scope of the tests is also a challenge, although it is recognised that it would be valuable to do so as these providers make up part of the potential attack surface. Moreover, it is recognised that there is a need to enhance integration of human behaviour into the testing. As one authority observed from the tests it has conducted, there is always an element of human compromise. This underscores the important role that human behaviour plays in cyber risk, which needs to be effectively captured in the tests.

Section 5 – Cross-border issues of red team testing

35. **Among the surveyed jurisdictions, although there is currently no formal arrangement for recognition of red team testing conducted under another jurisdiction's framework, authorities may be willing to consider exempting firms from local requirements if they fulfil certain conditions.** Most authorities are willing to consider such red team testing provided the foreign requirements are deemed equivalent to the local requirements. More specifically, the local authority will need to be satisfied that the scope, coverage and conduct of the tests under the foreign framework are adequate given the financial institution's local operations and risk profile. This may involve checking the credentials of the test provider or, alternatively, recognising the credential checking process in the foreign jurisdictions. Process-wise, a financial institution can apply for exemption from the authority to conduct separate red team testing if it satisfies the local requirements. While there are clearly operational efficiencies to be gained by firms if authorities can establish formal mutual recognition arrangements for red team testing requirements, this may be difficult to achieve in practice due to the different emphasis in the different frameworks to fully reflect the local cyber ecosystem.

36. **Given that cyber risk transcends jurisdictional borders, coordinated cross-border red team testing by financial institutions with cross-border operations could be beneficial.** An attack surface covers an entire organisation regardless of geography, and attackers can attack any part of that surface. Therefore, without looking at the cross-border dimension, it may not be possible to capture certain potential real-life attack scenarios. A coordinated cross-border red team testing framework could facilitate consistent testing of cross-border firms and minimise unnecessary duplication of efforts by both firms and financial authorities. This is especially useful for financial institutions with centrally managed infrastructures operating in jurisdictions with compatible frameworks. For example, the TIBER-EU framework is explicitly designed to facilitate cross-border red team testing within EU jurisdictions, in order to avoid the need for multiple testing by institutions in the region. Discussions are under way among financial regulatory authorities in several advanced economies to coordinate cross-border red team testing. In practice, firms by themselves may conduct cross-border red team testing even without formal arrangements in place among the regulatory authorities. In such cases, it is desirable if those firms inform financial authorities in the relevant jurisdictions beforehand.

37. **Despite the benefits of cross-border red team testing, there are significant operational, technical and legal challenges in conducting such activities in practice.** Some are of the view that operational and legal challenges may be harder to address than the technical challenges. Operational challenges include putting in place arrangements that would establish trust among the authorities involved, including having a secure platform for exchanging information. Effective coordination

arrangements must also be put in place not only for the actual conduct of the test but also in order to keep the international intelligence community informed. A cross-border test could generate international intelligence traffic that could raise red flags in the community, so coordination arrangements must be put in place to make clear which intelligence is test-related. Legal challenges, on the other hand, include differences in legal regimes for cross-border sharing of information as well as data protection and confidentiality. Technical challenges, meanwhile, include coming up with scenarios that would be appropriate for the different participating jurisdictions and reconciling differences in regulatory requirements or expectations for red team testing. Table 3 provides a non-exhaustive list of these challenges.

Challenges related to cross-border red team testing Table 3

Challenge	Example
Operational	• Firms and authorities having sufficient time and resources to plan and conduct tests. • Coordinating and achieving trust among the different authorities. • Managing information (test-related intelligence) flows within the international intelligence community. • Having a secure platform and clear protocols to exchange information among authorities in different jurisdictions.
Technical	• Designing scenarios that are relevant to the specificities of the cross-border firm and the jurisdictions in which it operates. • Agreeing on the objective of the activity among the different authorities, and correspondingly the breadth and depth of the red team testing. • Differing (and potentially conflicting) regulatory requirements on red team testing in the different jurisdictions.
Legal	• Data protection and confidentiality requirements. • Legal impediments in exchanging sensitive firm-specific information across jurisdictions.

38. **Financial authorities can contribute to addressing some of the challenges in conducting cross-border red team testing.** For example, the authorities can coordinate the activity through early preparation by establishing the objective of the red team testing, its parameters, applicable requirements in each jurisdiction, and communication protocols including mutually agreeable mechanisms for sharing information and engagement with firms. Cross-border coordination for red team tests would also need to be respectful of differences in certain test elements between frameworks. One way to address this is to follow the framework with the strictest requirement in conducting the cross-border test.

Section 6 – Conclusions

39. **Most of the surveyed jurisdictions have red team testing frameworks in place, although the objectives and implementation details may differ.** The frameworks apply typically to large or critical financial institutions, but authorities may have discretion to include other financial institutions. In a few jurisdictions, the frameworks are mandatory for domestic systemically important financial institutions, and banks deemed risky from a supervisory perspective. The frameworks also differ in terms of whether threat intelligence and red team test providers must be external to the financial institution, accredited and formally assessed.

40. **In general, all frameworks specify the following steps in the conduct of red team testing:**

- Define the scope and establish risk management controls for the test.
- Procure threat intelligence and red team providers.
- Gather threat intelligence.
- Conduct the actual red team test.
- Analyse the outcome of the test and put in place a remediation plan, where necessary.
- Share the lessons learned with other players in the financial system.

41. **International standards relating to the cyber resilience of financial institutions have raised the bar in terms of defining the expectations on firms.** Central to this is the use of red team testing as one of the tests that firms can undertake to assess resilience against realistic cyber attacks and strengthen their cyber resilience posture. Other benefits of red team testing for firms include having a methodology to establish remediation plans to address identified weaknesses; being able to better organise and process threat intelligence; fostering closer cooperation among different units; promoting stronger security awareness and culture; and raising accountability of the board and management on cyber risk management. For supervisors, red team testing provides for a mechanism to better understand financial institutions' cyber resilience posture, as well as to identify common weaknesses and strengths across the industry.

42. **Nevertheless, there are challenges that need to be overcome, and certain facilitating conditions appear to be instrumental in supporting effective implementation of red team testing.** Such conditions include a conducive governance structure, an engaged board of directors, a supportive risk culture and, critically, the availability of sound professional skills. A key challenge in many jurisdictions relates to insufficient numbers of adequately qualified threat intelligence and red team providers. Interestingly, explicit and formal assessment of threat intelligence and red team providers is not common practice. In certain jurisdictions, an accreditation framework has been established to boost local capacities. However, there is a view that shortage of cyber expertise is a short-term problem that will be tackled through market forces and maturity over time. Another culture-related hurdle to overcome is getting firms and authorities to view a red team test as a "learn and improve" rather than a "pass or fail" exercise. Other challenges in connection with red team testing include the high cost to firms, trust among the involved parties and data confidentiality.

43. **To take red team testing to the next level, consideration could be given to addressing the legal, operational and regulatory challenges in coordinating cross-border red team testing for internationally active financial institutions.** Extending red team testing beyond jurisdictional borders is important to minimise potential cyber resilience blind spots given that cyber attackers could attack any part of a financial institution's attack surface. In addition, cross-border technological dependencies could give rise to systemic implications should cyber attackers succeed in exploiting vulnerabilities that could trigger such chain events.

44. **Going forward, financial sector authorities may wish to clarify how red team tests fit within their strategies to improve the cyber resilience of financial institutions.** This will help provide regulatory certainty to firms and prompt concrete actions to improve their cyber resilience postures. Consideration should also be given to clarifying how red team tests fit within an institution's cyber resilience framework, which in turn should be coherently considered in its enterprise-wide risk management framework. Given that red team testing approaches are still evolving, it is important that authorities continue to assess the effectiveness of their frameworks and use the lessons learned from each test to improve the overall cyber resilience of the financial sector. In the course of this journey, authorities may need to enhance cooperation with other relevant authorities and parties in order to enable effective implementation of the frameworks.

References

Association of Banks in Singapore (2018): Red Team: Adversarial Attack Simulation Exercises: Guidelines for the Financial Industry in Singapore, November.

Bank of England (2016): CBEST Intelligence-led Testing: CBEST Implementation guide.

Brangetto, P, E Çalişkan and H Rõigas (2015): Cyber red teaming: organisational, technical and legal implications in a military context, North Atlantic Treaty Organization.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016): Guidance on Cyber Resilience for Financial Market Infrastructures, June.

Crisanto, J C and J Prenio (2017): "Regulatory approaches to enhance banks' cyber-security frameworks", *FSI Insights on policy implementation*, no 2, August.

European Central Bank (2018a): TIBER-EU Framework – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, May.

——— (2018b): TIBER-EU Framework – Service Procurement Guidelines, August.

——— (2018c): TIBER-EU Framework – The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test, December.

Financial Stability Board (2018): Cyber Lexicon, November.

Group of Seven (2018): G7 Fundamental Elements for Threat-led Penetration Testing.

Group of Twenty (2017): Communiqué, G20 Finance Ministers and Central Bank Governors, March.

Hong Kong Monetary Authority (2016): Cyber Fortification Initiative, December.

——— (2018): Implementation of Cyber Resilience Assessment Framework, June.

——— (2019): Update on Enhanced Competency Framework on Cybersecurity, January.

Lockheed Martin Corporation (2015): Gaining the advantage: applying cyber kill chain® methodology to network defense.

Massachusetts Institute for Technology Research and Engineering (MITRE) (2017): Finding Cyber Threats with ATT&CK-Based Analytics, June.

Saudi Arabian Monetary Authority (2019): Financial Entities Ethical Red Teaming, May.

United Kingdom Ministry of Defence (2013): Red Teaming Guide, Second Edition, January.