Red Team: Adversarial Attack Simulation Exercises

Guidelines for the Financial Industry In Singapore

Version 1.0

November 2018

The Association of Banks in Singapore

Table of Contents

1 Executive Summary

Cyber security attacks against organisations such as financial institutions (FIs) are evolving rapidly in scope, complexity and sophistication. To address this risk, FIs deploy layers of defensive measures, solutions and controls to reduce their exposure to attacks and improve their response readiness. Offensive simulation exercises complement the defensive layers to assess the effectiveness of defences and improve the security team's preparedness to detect and respond to incidents.

Adversarial Attack Simulation Exercises (AASE), often referred to as Red Team (RT) exercises, are sanctioned, planned, risk-managed and objective-driven cyber security assessments that simulate highly sophisticated targeted attacks against an organisation.

The objectives of AASE are to assess and enhance the resilience of FIs against sophisticated attacks. In order to efficiently allocate their resources to the unique threats they are facing, FIs are encouraged to create scenarios for their attack simulation by identifying the most likely adversaries and the attack vectors through threat modelling. The goal of these exercises is to assess the capability of a FI to prevent, detect and respond to cyber-attacks that may impact Critical Functions or business continuity. To achieve this, these exercises simulate a full end-to-end cycle of a cyber security attack, replicating actions and procedures utilised by real world adversaries with a high level of intent, sophistication and capability.

This document provides guidelines for the financial industry in Singapore for executing such exercises. It contains the guidelines and best practices to help organisations plan, execute and report of such exercises.

2 Introduction

AASEs are designed to challenge a FI's cyber security defences by modelling and then executing attacks based on real adversaries' Techniques, Tactics and Procedures (TTP). Scenarios are designed to be as realistic as possible, and may target the FI's People, Processes and Technology with the intent to compromise organisation's Critical Functions (CF). The primary goal of the exercise is to assess the organisation's ability to prevent, detect and respond to cyber-attacks and discover potential weaknesses that may not be identified through standard vulnerability and penetration testing methodologies.

This guideline is intended to support FIs within Singapore but may also be used by other organisations to plan and conduct such exercises. The document provides guidance on best practices and recommendations on how to adopt them partially or in full, and depending on the maturity of the FI's capability in conducting these exercises.

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

It is expected that the objectives, test scenarios and the report structure will be tailored according to the FI's scale, operations, external threat landscape and risk appetite.

3 Exercise Benefits

An adversarial attack simulation methodology provides a more authentic and holistic view of a FI's resilience.

By simulating realistic attacks during the exercise and taking into consideration the relevant threat landscape and potential adversaries, the following benefits can be achieved:

- An assessment of the organisational resilience against adversarial attack techniques, tactics and procedures.
- Identification of weaknesses in security controls and associated risks not detected by standard vulnerability and security testing methodologies.
- An assessment of the FI's security incident management and/or crisis management response and processes.
- A safe, controlled opportunity to identify and enhance the security posture of a FI reducing risk of cyber compromise.
- 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.
- Provide pragmatic direction to the involved stakeholders as well as confidence in an informed post-activity short, medium and long-term security strategy.

4 Definitions

The section below outlines key definitions and terms used when conducting adversarial attack simulations.

Term	Definition
Adversarial Attack Simulation Exercises (sometimes referred to as Red Team Exercise)	AASE provide a realistic picture of the FI's capability to prevent, detect and respond to real adversaries by simulating the TTPs of real-world attackers to target the people, processes and products technology underpinning the Critical Functions in a FI.
Attacker (sometimes referred to as Red Team)	An Attacker is an individual or a team who is employed or contracted by an organisation to simulate the attack TTP of a real-world adversary based on intelligence about prevailing and/or probable cyber threats and incidents to stress and provide guidance with regards to enhancing organisational resilience, utilising goals set in the scope of the exercise. For an effective exercise, ideally, the skills and capability of the Attackers should be matched to those expected of real-world adversaries as closely as possible. The provider selection section provides some guidance on selecting a provider with adequate capabilities.
Concessions	Concessions are a method of deliberately altering the course of the exercise by providing explicit, agreed assistance to the attacking team to achieve the goals of the simulation. To obtain maximum value from the simulation exercise, concessions may be given in order to enable the exercise to proceed further, more rapidly, and/or without full disclosure of the exercise. Concessions may be given to support the following: ▪ Simulate the passage of a very long period (for example reconnaissance time). ▪ Skip over an undefeated control. ▪ Delay or hinder the organisational response to enable further attack scenarios to be progressed. ▪ Restrict broad disclosure of the exercise while the simulation is

	still active. Simulations of altered conditions arising from concessions granted must be documented in the reports and considered when assessing the security control efficacy. Concessions may range from providing information about assets to providing hardware or software resources that can be used during the exercise. Some typical examples of concessions are administrative or plain user accounts, network diagrams, network access or laptops, data flow information, etc.
Critical Functions	Critical Functions are business functions or services that if compromised would significantly impact business continuity, affect the reputation of the FI or cause financial loss. These Critical Functions generally represent the greatest opportunity for real-world adversaries who are motivated by financial gain, information or intellectual property theft, and/or a desire to inflict business disruption.
Defender (often referred to as Blue Team)	A Defender is an individual or a team who is employed or contracted by an organisation to detect and/or prevent a cyber-attack and respond to one when it happens. This virtual team would typically include all resources in the FI's Security Operations Centre, incident response teams, and other technology infrastructure support functions.
Exercise Escalation Path	The Exercise Escalation Path represents the chain of control for any issues faced during the exercise where the Exercise Director would be obliged to inform the senior technical management of the organisation (such as the CISO, CIO or CTO, depending on the organisations).
Exercise Director	The Exercise Director is employed or contracted by a FI to oversee the development, execution, review and/or approval of the exercise. The role has primary accountability for managing the delivery of the exercise, and operational risks arising from an adversarial attack simulation exercise being conducted on the production environment. The Director would be able to understand the technical details associated with the attacks and its possible risks and potential

	consequences. The definition of the qualifications required by the Director will not be articulated for this document. More broadly, the Director is expected to have intimate knowledge of the FI's infrastructure and applications.
Exercise Working Group (Attackers + Exercise Director)	The Exercise Working Group is a team that comprises the Attackers, and the Exercise Director. As the Exercise Working Group will be heavily involved throughout the planning and execution phase, they must ensure that all information regarding the AASE remains strictly confidential to avoid "tipping off" the Defenders. The Exercise Working Group may, however, ensure that senior stakeholders whose systems are being targeted are aware of the exercise and are positioned to provide required authorisations/approval for the planned attack teams' activities during the exercise.
Facilitators	Facilitators are employees of the FI in key positions that can assist the execution of the exercise by providing support to the simulated Attacker/Red Team to enable the exercise on request from the Exercise Director. This support is provided by way of pre-approved and pre-defined concessions such as approval to execute a specific command or to produce and release other supporting documentation/resources. Facilitators may be personnel from the business functions or IT support, and while they are aware of their obligations to assist with an exercise, they are not aware of the details of the exercise, overall objectives, or the progress of an active simulation. Given the potential added privileges granted to the Exercise Director, all actions must be thoroughly documented, and pre-approval should be sought from senior management during the preparation phase.
Letter of Engagement	A Letter of Engagement is to document the exercise that is commissioned, sanctioned and authorised by the FI. It should be signed by the sponsoring executive or senior management, and it should briefly describe the intent of the test, the extent of involvement of the testers, and instructions on how to authenticate them for their authorisation during a potential investigation. This can be useful in situations where the testers need to prove their intent if they are apprehended by security staff.

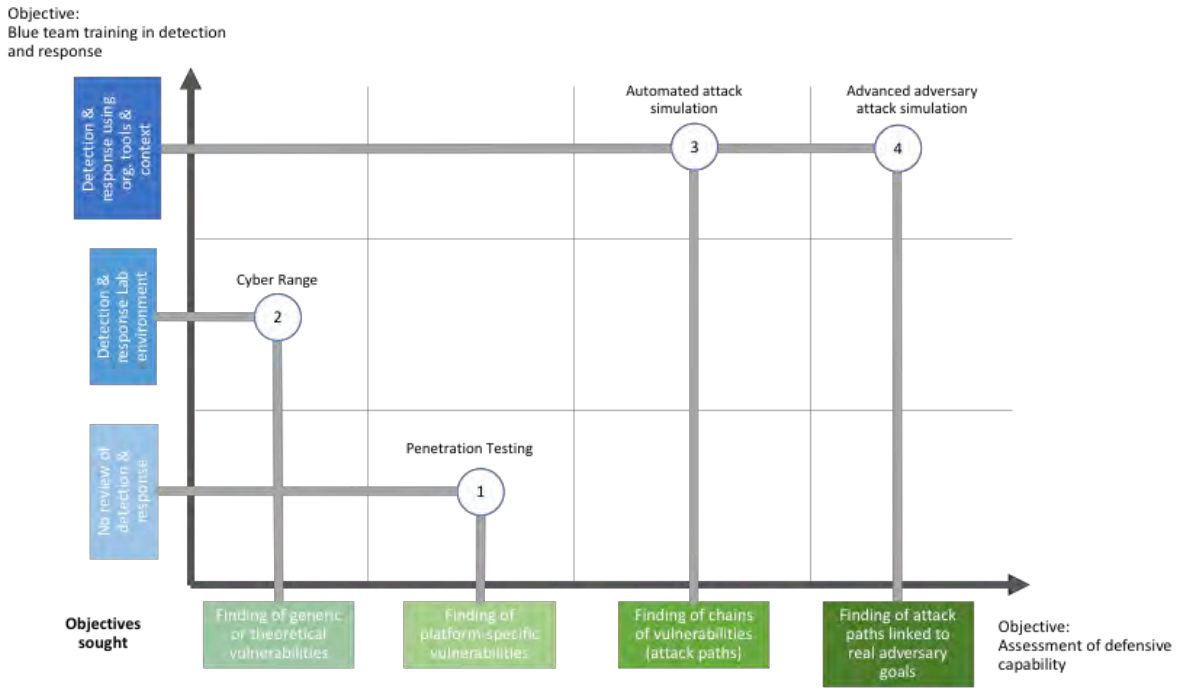
Organisational Escalation Paths	The Organisational Escalation Paths represent the different chains of control for any operational issues encountered, as part of the FI's standard business practices, where the FI's staff would inform the organisation's senior management of the problem. During the exercise, certain actions may be escalated, such as security incident when the Defenders would detect potential suspicious activity, or when the business operational team would detect suspicious transactions are being created or authorised. In some cases, the Exercise Working Group may want to ensure someone in the normal organisational escalation path, sufficiently senior, can intercept the escalation and jointly decide the next steps with the Exercise Director. More details about this setup are provided in the Methodology section.
Threat Intelligence	Threat Intelligence is the process whereby analysis is performed against real-world threats that would potentially apply as a threat to the FI. Threat Intelligence is supported by a variety of sources including internal intelligence gathering, public and proprietary information feeds, and security intelligence sharing platforms.
Threat Modelling	Threat Modelling is the process where the outputs of the Threat Intelligence process are used to generate likely attack scenarios that can accurately simulate real-world cyber security threats under operational conditions. The threat model report defines profiles of the likely threat actors expected to target the critical functions and the underpinning systems of the FI. It also provides detailed scenarios, and methods that the threat actors are likely to employ when targeting these systems.
Target Organisation	The Target Organisation or "organisation/FI", in this document, refers to the target of AASEs and the potential target of real-world attackers.

5 Getting Started with Adversarial Attack Simulation

Adversarial attack simulations serve to complement other forms of security testing (e.g. code review, vulnerability assessment, penetration testing) and should be incorporated into the security testing program of an FI as it grows in its maturity level.

Depending on the level of maturity and scale of a FI, the FI may conduct AASE in parallel with other additional exercises to assess its organisational resilience against cyber threats.

Different offensive initiatives are available for FIs to assess their capacity to defend and respond to attacks, each providing a different value in terms of defensive objectives. It is important to be aware of differences between AASEs and other types of security testing. FIs should take note of their current cyber resilience maturity when planning advanced adversarial attack simulations exercises. Furthermore, it is important to note that operational and legal considerations may place some limitations on the ability for an exercise to fully recreate a real-world attack.



5.1 Organisational Maturity in Conducting Adversarial Attack Simulation Exercises

The table below provides some recommendations to establish a testing program based upon the FI's maturity and scale of operations, and a pathway for increasing the sophistication of these exercises over time.

Maturity	Description	Recommended Approach
Low	• Limited attack surface in terms of number of systems, business operations, and organisation scale • No/limited prior exercises conducted • Some experience with standard security and vulnerability testing methodologies • Limited security testing on primarily non-production systems • Table top exercises may have been conducted previously • No systematic review conducted to make improvement on the capability to detect and respond to events	• Familiarisation with the concepts of AASEs • Identify intelligence sources (internal/external) as an input to planning phase • Execute planning phase • Conduct initial table top exercise • Review outcomes of the table top exercise and plan the next iteration of attack simulation to improve the security testing capability. • Plan for adversarial attack simulation exercise as a proof of concept and/or in response to specific security threats
Medium	• Conducted adversarial attack simulation • Ad hoc engagements of 3rd parties to carry out exercises	• Alignment with the exercise guidelines wherever possible • Plan for conducting periodic exercises
High (ultimate target and scope of this document)	• Periodic exercises planned and conducted • Dedicated budget and/or resources for exercises • Internal functions established and/or dedicated to AASEs	• Extensive adoption of the simulation guidelines • Add more iterations of the exercise focusing on building abilities to counter every action taken by real attackers

	• Complex and sophisticated scenarios • Security controls uplift/remediation driven through outcomes of exercises	

5.2 Differences with Penetration Testing

Some of the key differences between Penetration Testing and AASEs are:

Penetration Testing	**Adversarial Attack Simulation Exercises**
Primary objective is to identify as many vulnerabilities as possible, in a limited scope.	Primary objective is to stress and enhance organisational ability to detect and respond to adversaries.
• Limited scope, asset-based technical assessment	• Objective-based, open-scoped, designed to demonstrate critical impact to a business or organisation. Targets people, process and technology
• Made known to all the stakeholders	• Covert. Only the Exercise Working Group is aware of the exercise
• Social engineering is not used	• Social engineering may be used
• Physical security will not be tested	• Physical security may be tested
• Execution aligned to industry-recognised technical methodologies	• Execution aligned to mimicking Tactics, Techniques and Procedures of real-world adversaries

5.3 Differences with Real Attacks

The key differences between Real Attacks and Adversary Simulation Exercises are: -

Real Attacks	Adversary Simulation Exercises
• Usually not time-bound	• Usually time-bound due to resource limitation granted in a project (but could be open-ended)
• Not bound by Law or Ethics	• Bound by Law and Ethics
• Uncontrolled by the target organisation	• Controlled by the target organisation, risk controls can be applied
• May use physical/psychological violence and extensive coercion	• Respects the integrity and well-being of employees and partners

6 Guiding Principles

The success of these exercises is guided by the following principles:

6.1 Exercise Goals

Exercise simulations should be based on the likely goals of real-world sophisticated adversaries.

AASEs are goals driven. The intent of the exercise is not to identify and report vulnerabilities a FI may have. The goals represent what real-world adversaries may want to obtain or understand by compromising a FI.

For example, a FI could be targeted by an adversary for financial gain and the objective could be to demonstrate an ability to perform a large unauthorised funds transfer. Scenarios will therefore be developed to include all the steps to reach that goal.

It is not necessary to rotate or vary goals for every exercise as threat intelligence or other information may indicate that real-world adversaries could still have the same motivation.

6.2 Exercise Secrecy

The scope, nature and timing of the exercise should be kept secret to adequately assess the effectiveness of security defences and response to cyber-attack scenarios.

The information related to the exercise should only be circulated and discussed within the Exercise Working Group for the duration of the exercise. The Defenders are expected to react to the simulated attack in the same manner that they would do when they detect real attacks. Keeping the scope, nature and timing of the exercise secret would therefore provide a more accurate assessment of the capability of the Defenders to prevent, detect or respond to real-world or simulated cyber-attacks.

6.3 Targeting of Live Critical Functions

Exercise scenarios should be designed to target Critical Functions of the organisation and in a manner that is aligned with the motives of expected adversaries (in the production environment).

Real-world adversaries are motivated to compromise Critical Functions to achieve maximum impact. Motives of adversaries can include business disruption, financial gain, and/or information theft. As such, the same functions should therefore be targeted by the Attackers in the exercise.

Given the purpose of the exercise is to stress and enhance the FI's current resilience to a real-world adversary, the exercise should be conducted against the live environment. Assessments in staged or otherwise non-live environments may influence the outcome of the exercise, and would not be representative of organisational cyber resilience against real-world threats.

Assessment in a live environment would include for example the exploitation of the staff cognitive biases, identification and exploitation of gaps within processes utilised by an organisation and subversion of existing business process or technologies within an environment.

6.4 Exercise Frequency

Exercises should be conducted periodically. In each iteration of the exercise, the scenarios and sophistication of the TTPs used could be adjusted with the

improvements made in the organisations cyber preparedness, security operations, as well as variations in the threat landscape.

Exercises should be conducted on a periodic basis. The frequency should be dependent on the efforts and enhancements made to increase organisational capability, which merit stressing in a real-world scenario. A recommended minimum is to execute an exercise at least once per year. Scenarios and goals need only be changed if Threat Intelligence indicates that the threat landscape has changed, or controls around Critical Functions vary.

The organisation should also develop a process to periodically review the frequency, based on the evolving risk and controls. Results and learning points from past exercises may also influence the frequency.

6.5 Exercise Duration

Exercise duration will be determined by the complexity of the attack scenarios, and the scale of the organisation being examined.

The duration of the exercise is considered during the planning phases and is based upon the perceived persistence, and operating procedure, of the adversary that the FI is looking to simulate. Typically, a large financial institution may operate a cycle of between four to six months for complex scenarios (inclusive of Threat Modelling). Smaller organizations with less complex IT environment may be able to complete table top scenarios, or very limited production testing over a shorter period of one to two months.

Some FIs may choose to test its defences through continuous adversarial attack simulations whereby the Attacker would be able to adjust their attack depending on the changes to the threat landscape. Exercises may also be open-ended (no defined timing but only closed upon achieving the goals).

At the end of each AASE, there should be a comprehensive evaluation from the adversaries' perspective of the FI's current prevention, detection and response capabilities, and a roadmap of on-going improvements over varying periods of time.

7 Methodology

Overview:

The typical methodology of executing AASE involves four distinct phases, with planning, attack preparation, attack execution and exercise closure.

The AASE starts with a “planning phase” where the scope of the assessment is defined and described, service providers are sought and a budget is set aside. An Exercise Working Group is formed and communication protocols are defined.

The second phase, “attack preparation”, involves the creation of scenarios based on the defined Critical Functions and exercise threat model.

The third phase, “attack execution”, is usually comprised of several sub-phases.

The final phase, “exercise closure”, is for reporting, cleaning-up, transferring knowledge, remediating and communicating outcomes at the conclusion of the exercise.

7.1 Planning Phase

Prior to the start of the AASE, careful planning is required to ensure that the exercise can be conducted effectively and with minimal risks to the FI.

It is recommended that the planning stage includes the following steps:

- **Define the key exercise parameters** including desired outcomes. This will affect the degree of secrecy required, the composition of the Exercise Director team, the escalation and cautions required, the data management, and lastly the selection of providers. Those parameters will impact the course and results of the exercise.

- **Determine the scope and duration of the exercise.** This will affect the number of goals that could potentially be achieved during exercise period. Given the focus of the exercise is to stress organisational resilience and controls, it is recommended that defined goals and objectives, where relevant, should cover both technical and business

controls by the FI. In addition, Critical Functions, which are important to the organisation should also be covered and tested.

- **Determine the participation model.** For instance, whether the exercise can be performed by the FI's own experienced staff, by external service providers or a combination of both. The exercise requires Threat Intelligence analysts to perform threat intelligence gathering and qualified Attackers to execute the attack (although both roles can be performed by the same, appropriately qualified person). It is recommended that these capabilities are provided by impartial parties, ensuring the integrity and realism of the exercise.
  - The planning stage should include the selection and procurement of the external services, if using.
  - The FI should only engage service providers that are reputable and have experienced persons to perform such exercises. Recommendations in selecting the right provider are detailed in Section 7.1.4 "Provider Selection".

- **Formation of the Exercise Working Group** that will oversee and direct the entire exercise. Members of the group should maintain secrecy throughout the entire exercise and not disclose the scope and plans of the exercise to persons outside of the group. To avoid any security alerts generated by the exercise from being escalated beyond what is necessary for the exercise (i.e. to law enforcement or government authorities), the Exercise Working Group should consist of members who are part of the Organisational Escalation Path, and would be informed of such escalations and are able to intervene where needed.

- **Determine the escalation process** and key persons for the escalation of any emergency issues encountered or caused during the exercise. If the escalation process and the key persons cannot be determined at the planning stage, it is acceptable to do so at the later stage after the Critical Functions that are in scope have been determined.

The decisions made during the planning phase are usually captured in the Exercise Preparation Report.

7.1.1 Goals and Scope

Scoping of the exercise should be performed by the Exercise Working Group, which typically involves both business and IT leaders, and should be led by the project sponsor, which will typically be the FI's CISO or its delegate. Scoping should include identification of Critical Functions within the FI that are likely to be targeted by real-world adversaries.

7.1.2 Defining Exercise Parameters

Defining parameters must be carefully agreed during the planning of an adversarial attack simulation exercise. These parameters are identified as key, since they will directly influence the realism of the simulated attack, and therefore the benefit of the overall exercise.

Determine the Degree of Secrecy of the Exercise

The first defining parameter is the degree of secrecy desired prior to and during the exercise. Higher levels of secrecy allow the exercise to demonstrate and validate actual and unfettered response of the FI to a cyber-attack, but such an approach can introduce additional operational risk e.g. high risk recovery actions or responses initiated in the production environment could result in prolonged outages to services and business disruption. Lower degree of secrecy tend to diminish the execution of detection and response capabilities and processes, and will influence or otherwise undermine exercise outcomes. FIs should determine the ideal degree of secrecy to allow adequate testing of their ability to detect and respond to threats, while minimizing risks of disruption to the FI's business. FIs should also plan recurrent exercises with higher levels of secrecy in subsequent iterations.

Select the Exercise Director and Exercise Working Group

Typically, the Exercise Working Group supplements and assists the Director in conducting the exercise, by observing, opining, and intervening where necessary. Regular meetings should be established within the Exercise Working Group to oversee the progress of the exercise.

The Exercise Working Group would usually consist of staff in key functions who are able to influence incident responses in cases where there is a need to alter the outcomes of the exercise, and other processes. The participants may include members of:

- Senior Management
- Risk Units (Business Risk, Technology Risk, Operational Risk, Cybersecurity Risk)
- Business Continuity and Crisis Management

- Incident Management
- Information Security
- Relevant Business and System owners
- Legal and Compliance

The Exercise Director should be able to decide, at every stage of the exercise, whether to proceed with an action, pause, or terminate the exercise. The Exercise Director should be qualified and sufficiently aware of both technology and business to make such decisions, and these decisions can be supported by the Exercise Working Group.

Define Exercise Data Handling Protocols

Data handling and management protocols should be established prior to the exercise commencement for the Exercise Working Group. These protocols must define how data exposed or acquired during the exercise should be handled (e.g. usage, data protection and retention).

Given the nature of the simulation, the Attacker may potentially gain access to the FI systems and data.

The protocols should limit access to this data by the Exercise Working Group, as its members may not be authorised to handle this data by their individual scope of roles. Access to acquired data should be managed, and the Attacker, should only present to the Exercise Working Group a subset of data sufficient to validate achieved goals. This subset can be produced from smaller samples of acquired data that has been redacted to remove sensitivity. Ideally, all data verification should be performed by the business owner of that data set, and whose scope of role includes having access to this data.

There should be an agreed protocol to adequately protect the data which the Attackers may have access to. The protocol should guarantee at minimum the same level of protection adopted by the FI, ensuring data is only available to the members of the Attacker group that are directly involved with the simulation, and that data is destroyed after the exercise. There should also be an agreed process to dispose data used during the AASE in a secure manner.

Assess the Impact to Production Systems and Operations

While creating the scope of the exercise, impact to the environment should be carefully considered with a thorough risk assessment. If the protential operational impact to specific

components in the live environment during an exercise is deemed to be unacceptable, the FI may consider performing the exercise on a simulated instance that is a close replica of the actual instance. However, the FI should be aware that performing the exercise on a simulated instance may limit the realism of the exercise, its results and reduce the overall benefits of the exercise. Hence, conducting the exercise in the test environment should be an exception rather than a norm as the results may not reflect the true security state of the FI.

Any parts of the exercise that are not performed on the live environment should be clearly documented with reasons in the report. For example, certain functions, assets or areas/zones can be designated as "no-fly zones" due to excessive risk involved with testing.

Operational impacts should also be considered arising from recovery actions or response taken during the exercise such as wiping endpoints or resetting passwords.

Establish the Budget

When budgeting for such exercises, the FI should consider the intended frequency, complexity, size of scope and duration of the exercises, as well as the cost of potential service providers.

Major business changes on the systems being attacked occurring during the exercise may increase the risk of unforeseen operational impact or reduce the effectiveness of the simulation. In this case, FIs should consider reviewing change plans with their IT Project Management Office or Change Management teams during the planning phase to avoid conflicting calendars.

Consider Engaging External Providers

While larger FIs tend to have their own internal specialised teams, external providers may be engaged to offer independent views on conducting the Threat Modelling and the simulated attack. Maintaining the same provider across exercises provides benefits, such as building deep understanding of strengths and weaknesses of an organisation akin to real-world adversaries, an organisation may be breached multiple times over a period of years to develop understandings and situational awareness – this can be simulated by utilising the same provider.

Engaging different providers may on the contrary offer different insights, perspective and TTP.

The FI should perform their own assessment to determine whether keeping or changing providers would enable it to achieve the intended outcome.

7.1.3 Risk Management

AASE should always be conducted against live production to assess real-world cyber resilience.

Depending on the approach, certain threat scenarios could involve high-risk activities, and once carried out on a production environment, could lead to uncontained impact resulting in damages greater than the benefit of the adversary simulation itself. Therefore, FIs should perform a risk analysis during the scoping phase.

If the assessment indicates that risks arising from testing in the real-world environment are deemed excessively high and could result in operational failure, certain elements of testing could be performed in staged environments to minimise impact. This approach however does not allow for an accurate reflection of the FI's security state and should only be used in circumstances of very high uncertainty of operational risk.

If such a simulated approach is chosen, high-risk activities can be conducted through coordinated actions on both the production and a replicated environment, i.e., obtaining access on the production and then, using the same level of access on the replicated environment, demonstrate the ability of altering critical business data. For example, when targeting a payment processing infrastructure, the Attacker could try to obtain access to the production environment but will not make changes such as submitting payment messages or creating new user accounts; instead, these activities will be carried out on a replicated environment with the same configurations and level of access that they had previously obtained in the production environment. While potentially close to the real-life environment, this arrangement should be clearly documented in the reports. This method allows for the execution of a goal when only technical hurdles or challenges remain, and cannot replace subversion of business controls (such as legitimate maker/checker processes). Proper oversight and escalation paths should be established before the start of the test to avoid any outages of critical infrastructure.

A number of key risks should be carefully considered during the planning phase of the exercise.

- **Business Continuity and Operational Risk**

  Due to the level of sophistication of typical attacks, there is an inherent accentuated risk of operational failures of infrastructure being assessed during the exercise. Hence, it is usually prudent to have members of Business Continuity or Crisis Management teams intimately familiar with the exercise, unless an objective of the exercise is to invoke and assess those specific processes.

  The Exercise Director and Exercise Working Group should be sufficiently informed and qualified to make decisions to drive the direction of the exercise should such events occur.

- **Legal and Regulatory Risk**

  Legal risks to be considered include legal liability as an outcome of adverse reactions to testing, such as failure to continue operations.

  FIs using systems or functions hosted by an external provider (i.e. Cloud service or external business function) should review the contractual terms of the service, as some providers do not allow attack simulations or require prior notice. The FI should consider these contractual obligations in the selection of Critical Functions to be tested.

- **Data Risk**

  The risks around data include data leakage, data destruction and alteration, and data unavailability.

  Should the risks be deemed acceptable by the FI, the Attacker could be requested by the Exercise Working Group to provide access to exercise execution logs. However, since execution logs contain information which may allow replay of the attacks, proper controls would need be implemented to ensure the security of this information.

- **Third-party Risk**

  Due to the nature of external engagements to perform AASE, third-party risk is one of the highest risk categories. Third-party risk may involve either malicious intent or reputational risk. It is important to mitigate third party risk by conducting adequate due diligence on service providers.

- **Malicious Intent.**

  There is a potential risk of the hired third party acting with malicious intent. Provisions should be made in the contractual phase that covers legal liability and indemnity in case of a potential rogue activity (e.g. theft of sensitive information, installation of malicious software like backdoors).

- **Insufficient Expertise of the Attackers**

  There is a risk of insufficient expertise of the provider, which could in turn cause events that would expose the FI to operational risks due to execution errors or negligence. The provider selection process is an important step and such risks should be duly considered.

- **Reputational Risk**

  All the risks as mentioned could potentially damage the reputation of the FI which can be mitigated with careful planning and execution.

7.1.4 Provider Selection

Due to the sensitivity of the systems potentially accessed, the provider selection process should at minimum seek assurances on appropriate testing methodology, data handling procedures, criminal background checks for its consultants, and adequate insurance and indemnity to cover legal liabilities.

When choosing a provider, its reputation, experience and references should be considered. Reputation can be established in industry collaboration forums, and references can be obtained from the potential provider. Providers should be able to demonstrate a real world understanding of sophisticated adversarial TTPs, which can be substantiated through publicised research, experience and recognised capability in responding to sophisticated cyber incidents.

7.1.4.1 Key Requirements of the Provider Organisation

Areas to consider when selecting third party AASE provider:

Methodology and Process

Having sound methodologies to be able to deliver technical certification and assurance related to AASE.

Reputation, Experience and Track Record

Providers should demonstrate strong capability such as holding recognised accreditations or having proven track record in analysing and replicating adversarial techniques from an offensive and defensive perspective, as well as providing evidence that they have helped to enhance their clients' the organisational resilience and defensive capabilities. A sound reputation in the industry across multiple geographies and jurisdictions is usually associated with a well-rounded provider.

Legal Coverage

FIs should ensure there are enough legal policies and procedures to be legally compliant, insured and indemnified for the type and nature of work. Specifically, considering the possibility of unintended damage to the systems being attacked, the FI should pay particular attention to mutual damages and liabilities, and to the provider's financial capacity to withstand such an eventuality.

Data Protection

Providers should have robust data management procedures that cover the protection of data at rest and data in motion, data retention and disposal procedures.

Background Checks

Due to the high sensitivity of the work performed, each provider should have standard practices of criminal record and other background checks for all consultants hired by them and trained in applicable regulatory compliance obligations.

7.1.4.2 Provider Obligations

In addition, it is important that the selected provider has considered the obligations below.

Compliance

The provider must comply with all relevant laws and regulations during the entire course of the exercise.

FIs should ensure that the provider is kept legally liable for its activities by stating such requirements in the Scope of Work, as well as through signing a Non-Disclosure Agreement.

Evidence Keeping

The provider should be required to keep only enough information as is required to provide evidence that specific exercise goals have been achieved and to reproduce the methods used to achieve the goal. They should not be allowed to manage and keep data belonging to the FI after the completion of the exercise, unless necessary for future exercises.

When third-parties are employed to conduct the attack, it is recommended that a secured storage space for data is set-up to securely store the data obtained from the FI's system. Such practice could facilitate the removal of data after the exercise.

Data Retention and Destruction

The service provider typically only needs to retain a small amount of artefacts eg, Screenshots it obtained during the exercise to produce the exercise a report, such as screenshots or small pieces of data. The contractual obligations may be specified to require the provider to only keep such reports for a limited amount of time. All other data acquired by the provider through the course of the exercise should be destroyed upon the exercise completion.

Physical Supervision

Depending on the exercise mode of operation and goals desired, certain elements of the exercise execution may benefit from real-time physical supervision by the Exercise Director, such as final execution of an action upon a goal, or physical access to premises. This should be considered in the planning stages.

7.1.4.3 Key Requirements of the Attacker (Threat Intelligence and Attack Teams)

Ideal characteristics include:

- Demonstrable technical skills, expertise, industry experience and competency relevant for the type of work provided, considering the industry and specific requirements, related to AASE.
- Demonstrable understanding of real-world adversarial activities.
- Ability to communicate well with senior management as well as technical experts.
- Education on the legal and compliance aspects to enable management of legal and regulatory frameworks applicable to clients and their relevant geographies and industries.

Threat Intelligence Team Specialist Requirements

The Threat Intelligence specialist should be able to perform with high level of confidence in all areas of threat intelligence, operational security, data collection, data analysis, intelligence production, scenario development and enrichment.

The threat intelligence specialist should be able to provide insights to the following questions:

- Who wants to attack the organisation?
- How to attack the organisation?
- Why do they want to attack the organisation? (What are the motives for the attack)
- When do they want to attack the organisation?

Attack Team Specialist Requirements

Specifically, the Attacker team should consist of specialists in Adversarial Attack Simulation with proven track record of:

- Mastering technical expertise in skills such as reconnaissance, perimeter breach, persistence, lateral movement and privilege escalation.
- Understanding and translating of sophisticated adversarial TTPs.
- A strong understanding of a wide breadth of typical preventative and investigative security technologies.
- Executing actions in both realistic test environments as well as real environments in a safe and legal manner.
- Strategic understanding of capabilities required to increase organisational capability to detect and respond to TTPs executed.
- Producing written documents and delivering presentations to all levels of business.

The Threat Intelligence and Attack teams should be able to demonstrate expertise in selecting and using the following artefacts for the exercise:

- Malware samples from known threat groups/actors (e.g. banking trojans, custom built ATM malware targeting specific protocols, command and control RAT, etc.)
- Command and Control ("C2") traffic and protocols (e.g. ICMP, DNS, HTTP/S, Direct TCP, etc.)

- Type of different infrastructure that can be used (e.g. Service provider, Known C2 hostnames and IP, etc.)
- Vulnerabilities that were exploited by known threat group/actors
- Known lateral movement and persistence techniques
- Operational hours
- Resources does the groups/actors have (e.g. Known 0days, Use of 1days, Dedicated R&D teams, etc)

7.1.4.4 Qualifications (including Certification and Accreditation)

The organisation and all its practitioners should hold accreditations or certifications that require practical demonstration of an advanced understanding of offensive and/or defensive security skills and the tactics, techniques and procedures utilised by real world sophisticated adversaries. These accreditations should also require that organisations, and practitioners, demonstrate an understanding of legal and operational security frameworks that apply to exercises of this nature.

There are accreditation bodies that provide certification and accreditation for this specific type of testing, and therefore such qualifications should always be sought. Upon request by the FI, the provider should supply the list of consultants that are assigned to the project, together with their biographies.

7.1.5 Concessions

Concessions that may be ceded during an exercise should be planned. These concessions can include software, hardware, people, processes, etc. Some examples could be:

- A dedicated Access & Identity Management ("AIM") administrator instructed to issue administrator or plain accounts on demand to the Attacker.
- A local IT person instructed to issue laptops or tokens on demand.
- Information about assets, processes, information systems, or key personnel attached to a function.
- Access control bypass to a network outlet that would otherwise be physically secured.

Some concessions can be provided upfront (e.g., assume an endpoint compromise will be successful and provide a laptop to be used for the exercise), and some can be issued during the exercise, at points where the Exercise Director establishes that they would be beneficial

for the outcome (e.g. deliberately distracting incident responders to prolong the attack vector's duration).

All concessions used, whether upfront or during the exercise, should be recorded, their impact analysed and reported in the Exercise Report.

7.1.6 Communications

7.1.6.1 General Awareness

An AASE's efficacy is highest when absolute secrecy is maintained in the FI. The major benefit of secrecy is that the entire response to the attack from all parts of the FI is genuine and organic, and therefore truly reflects the shape and form of the incident response. However, in AASE where secrecy was not preserved, the information leaked impacted negatively the behaviour of the incident response teams substantially and may compromise the benefits of the exercise. (Refer to the Secrecy Section)

7.1.6.2 Use of Code Names

To protect the secrecy of the exercise, the Exercise Working Group should use code names to refer to the exercise utilising terms that do not reveal the existence or nature of the exercise.

7.1.6.3 Stakeholder Management

As the AASE is a holistic approach to test the cyber resilience of an entire FI, the organisation's Board of Directors should be fully supportive of the principles, goals and implementation of the exercise. These duties are typically delegated to the CISO, CIO, or a senior executive on behalf of the Board. The Board, or sponsoring management, should be apprised of the intent of the exercise and the final outcomes. The senior management should receive and approve the final report and commit to remediation efforts via a management action plan.

7.1.6.4 Regulatory Disclosure

Financial Institution regulators in certain countries require some form of AASE to be executed periodically, while others suggest it or are silent. It may be prudent to advise the regulators of the intent to execute such exercises upfront. It should also be noted that in certain cases some adverse reactions may occur which would impact the FI's ability to operate as required, and may even require actions such as regulatory notification.

7.2 Attack Preparation Phase

To form realistic scenarios, FIs should determine what are the functions that are critical to them – the functions that if compromised would impact the continuity of the business, affect the reputation of the organisation or cause financial losses. These Critical Functions represent what adversaries may be after, for their benefit or the FI's detriment. Attackers are modelled after known real-world adversaries by listing their capability and intent, and identifying the most credible or those potentially representing an imminent threat to the FI. The combination of these two items will help to generate the scenarios that are most probable, together with associated goals for each of the scenarios.

7.2.1 Critical Functions Identification

The Critical Functions should ideally be already identified by the FI on a regular basis, but can be done at this stage if not determined earlier. The list should be designed in a way that the potential of compromise of these functions would lead to significant financial, reputational or regulatory risks to the FI. They would usually include functions that influence the movement of funds, trading, or functions that store or process a significant volume of confidential information.

7.2.2 Threat Modelling

After identifying the Critical Functions, the FI should perform threat intelligence gathering to determine the probable Threat Actors who will target the identified functions/assets and the TTP that they will use. FIs should gather and analyse threat intelligence from generic threat intelligence and targeted threat intelligence sources. Threat intelligence gathering can be performed by Threat Intelligence analysts who are either the organisation's own experienced staff or from external service providers.

7.2.2.1 Generic Threat Intelligence

Generic Threat Intelligence refers to threat intelligence information that is not specific to any particular FI but are threats that are generic to all FIs within the same industry or geography. Information of known Threat Actors and their TTPs can be obtained from sources such as publicly available threat intelligence reports. Publicly available exploits and tools, recently related vulnerabilities, and TTPs used by Threat Actors in recent compromises are good sources of information of how Threat Actors would compromise the identified functions and assets. The ATT&CK framework, public collection of known TTP can be useful too (link in the References section).

7.2.2.2 Targeted Threat Intelligence

To enhance the effectiveness of the exercise, FIs are recommended to perform targeted threat intelligence analysis that is specific to their environment, to identify the high risk and highly probable TTPs and Threat Actors. Targeted threat intelligence analysis should identify potential threat actors that are most likely to pose a threat to the organisation and should identify the TTPs that are most likely to be used in such attacks. This information should be further reinforced by the FI's own threat intelligence. It is often difficult for an external threat intelligence provider to have information on on-going attacks that model the current threat landscape of a specific organisation.

7.2.2.3 Target Reconnaissance

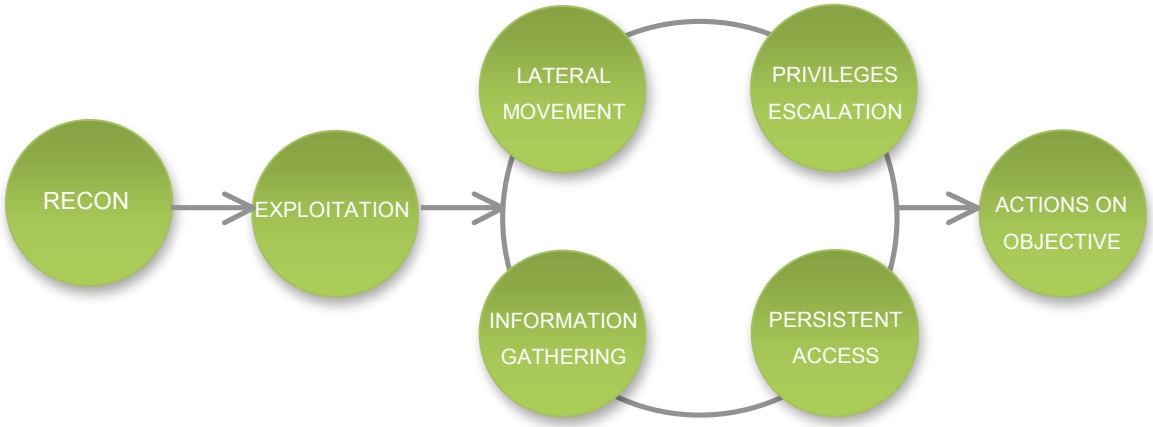
Target Reconnaissance is important for the Attacker to know more about the targeted organisation FI. An extensive amount of information will need to be assembled about developing a company profile, such as gathering a list of potential phishing campaigns and security controls to bypass, the key systems to target, the list of personnel or suppliers, the details about the organisation and its image, the technical infrastructure details, and other technologies. With this information, the Attacker will then be able to target specifically the organisation by, for example, sending specially crafted spear phishing emails with a high chance of getting the staff to open and the payload (malware) executed. All the information collected will be presented in a structured manner in the Target Reconnaissance report.

7.2.3 Attack Scenario Creation

Attack scenarios are created by the Exercise Director together with the Attacker by using the generated Threat Intelligence information to determine the most probable steps that real-world attackers would use to compromise the identified Critical Functions. It is recommended that several attack scenarios are employed in each exercise, as they would likely have overlapping components that could then be reused, thus saving time and budget.

Attack scenarios should also include criteria of what constitutes a successful compromise of the critical function. For example, where the target is a payment processing gateway, the FI may deem that the attack is successful based on the Attacker's ability to gain access to payment users' credentials and their access to the payment systems, instead of requiring the Attacker to fully demonstrate an actual fraudulent transfer. In other cases, the end-to-end demonstration may be required to test the effectiveness of all controls including the payment authorisation, the reconciliation with the logs as well as the various limits and alerts that may have been put in place. Together with the scenario, the Exercise Log Report will contain the initial plan to target these Critical Functions, to be revised during the course of the exercise based on the obstacles that the Attacker will face and the solutions to overcome them.

7.3 Attack Execution Phase



The execution phase involves the execution of the attack on the identified Critical Function based on the attack plan and scenarios that are formulated in the previous phase. During the attack execution phase, the Exercise Director should closely monitor the progress of the exercise and supervise the Attackers. While it is recommended for the Exercise Director to have full supervision at all stages, his involvement at certain stages where there is no impact such as reconnaissance can be reduced to a "keep informed" basis.

All steps taken by the Attacker and their observations should be continuously captured in the Exercise Log Report with the level of details determined in the requirements during the preparation phase. The Execution Log Report will also contain changes of plan, use of concessions and relevant approvals provided by the Exercise Director. As mentioned in the Risk Management Section, sharing the details of the attack with the Exercise Working Group carries a risk should the content be exposed unwittingly to either the Defenders or a real-world adversary.

To reduce risks during the attack execution phase, the "test/halt engagement model" should be applied.

7.3.1 Test/Halt Engagement Model

AASEs are a risk-based approach to holistic systemic testing. Simulated attacks are planned and analysed before they are executed, therefore the fallout and consequences can be predicted and minimised. These exercises typically consist of high risk activities, so the attack plans should be carefully analysed before approving them.

Once the exercise has begun, the Exercise Director should be in supervision of the efforts and is able to decide whether a particular attack path should be pursued, paused or diverted,

or if the entire exercise should be paused or terminated, depending on desired outcomes and potential adverse reactions.

Publicly exposed vulnerabilities

In the event where high-risk security vulnerabilities that pose immediate threats to the FI are identified by the Attacker during the exercise, the Attacker should inform the Exercise Working Group immediately. Examples of such high-risk security issues may include vulnerabilities allowing arbitrary code execution in internet-facing systems. The Exercise Working Group should determine whether such a finding would need to be escalated for remediation immediately, as this kind of escalation might compromise secrecy of the ongoing exercise. If such a situation occurs, access to the system is given to the Attacker to assume that the vulnerability would have been successfully exploited.

Evidence of prior compromise

If the Attacker discovers evidence or indication of prior compromise during the course of the exercise, they should immediately escalate such findings to the Exercise Working Group for investigation and deliberation on the future course of the exercise. The FI should seek to complete the incident response with regards to the said findings immediately, before continuing to pursue goals of the exercise, even if this requires halting or pausing of the exercise.

Attribution of TTPs during the exercise

If the exercise is designed such that the Exercise Director has insight into the incident response processes of the FI, then the Exercise Director should be able to identify incident notifications that are related to the exercise. There should be a hotline made available to the Director by the provider that can be used to validate and attribute TTPs observed in incident notifications that point to attacks made by the Attacker. This can be used by the Exercise Working Group to potentially intervene, either to diffuse or to delay/alter the incident response, should this mode of exercise be chosen.

A typical attack is not necessarily linear but will often involves repeating some of the following stages based on the position of the Attacker.

7.3.2 External Reconnaissance and Perimeter Breach

A reconnaissance is performed by the Attacker from outside of the perimeter, to find entry points into the target FI. This consists of discovery exercises, to identify potential weaknesses within external infrastructure and identify legitimate services provided by the FI.

Adversaries will also review legitimate sources of information, where information may have been inadvertently disclosed or intentionally disclosed (job descriptions as an example). This information is used to inform further stages of the exercise.

Entry points typically include (but are not limited to):

- Physical breaches
- Infrastructure breaches
- Social engineering (phishing, vishing, etc.)
- Supply chain attacks

The Attacker may choose to adopt techniques to bypass security controls and obtain access to corporate portals used by employees that may be externally accessible.

7.3.3 Lateral Movement

Adversaries will typically look to move between, and gain access to, various systems within an environment. This process typically involves the compromise of further systems or processes until an adversary has access to systems deemed and believed to be necessary for the success of the simulated adversary's objectives. Access to further systems can assist adversaries in:

- Increase level of access
- Evade detection
- Obtain further situational awareness and information
- Gain further perspectives on the network

Systems typically targeted for lateral movement can include:

- Asset management systems
- Anti-virus management systems
- Software delivery mechanisms

The Attacker may choose to adopt some of the above techniques during the exercise.

7.3.4 Internal Information Gathering

Adversaries will perform internal reconnaissance in order to achieve situational awareness and inform further stages of the exercise.

7.3.5 Privileges Escalation

Adversaries will typically attempt multiple escalating privileges methods to other systems or users on roughly the same level (horizontal privilege escalation) and higher privilege users or system (vertical privilege escalation). This should be performed in a way that mimics real-world advanced targeted breaches.

7.3.6 Persistent Access

Adversaries will try to maintain persistence upon breaching a network, utilising different methods of persistence in order to avoid eradication.

The type of persistence techniques that may be used depend on the environment, taking into account relevant controls.

7.3.7 Action on Objectives

Adversaries will proceed with the attack after he is satisfied that he has the resources and the right condition to perform the attack.

7.3.8 Directing the Attack (Escalation Path - Chain of Control)

The Exercise Director has the oversight of course of actions of the Attackers and can alter the course of actions of the Attackers or even alter the environment and situation if deemed beneficial for the outcomes of the exercise, or if the potential risks and consequence is high should there be a breach.

7.3.9 Use of Concessions

Concessions can be used by the Exercise Director to alter the course of the exercise. When used, they should be documented and reported.

7.4 Exercise Closure Phase

The exercise should be called to a close when either all steps of the attack have been successfully executed, or when the planned timeline has ended.

7.4.1 Clean-up and Tactical Vulnerability Containment

The primary objectives of clean-up activities and tactical vulnerability containment, conducted based on the information provided in the final report, are to remediate immediate issues found during the exercise, as well as eradicate any left-over attack tools and artefacts.The targeted FI should work with the Attacker to revert the environment to a secured state .

7.4.2 Defence Report and Reconciliation

The Defender's report is a document that reconciles the attack phases against the corresponding defence events or actions, if any. This report should identify all aspects of the exercise where the attack was detected, observed, reacted upon, tracked, contained and eradicated, or lost sight of. This reconciliation should be used to identify security controls, either missing or in need of improvement, that would otherwise have prevented or detected the attack.

7.4.3 Attack/Defence Joint Replay

A joint post-attack exercise can be organised to enable a step-by-step replay of the attack, either as a table-top or lab exercise for the Defence team's learning benefit, or in the actual live environment, to demonstrate failed controls in real-time.

In addition, the replay could include some hypothetical attack simulation for the benefit of the Defenders. The Attackers would then explain other steps they could have taken following another path and the steps they would have taken if the Attackers had more time or resources.

Lastly, the replay offers an opportunity for the Attackers and the Defenders to provide an opinion on the various activities performed throughout the exercise as potential improvement points. The Attackers could also offer an opinion on the performance of the Defenders, as a comparative analysis with similar organisations the Attackers worked with, should the Attackers be a third-party provider.

7.4.4 Final Reports and Recommendations

The Attacker will produce the Final report, providing an analysis of the FI's resilience and capabilities. It will include security strengths, comprehensive analysis of organisational capability, with recommendations for remediation and enhancements. This report will also contain the methodology, evidence of goals achieved, details of the attack path undertaken and the concessions, if any, used.

7.4.5 Strategic Remediation Management Action Plans

The FI should formalise a remediation timeline based on the final report, along with the organisation's risk appetite and compensating controls. The strategic remediation may involve items such as process changes within the FI, tightening of security controls, additional investments, end-user security training, architecture redesign, etc. The risk assessment should take into consideration the sensitivity of the data residing in the systems and the location of these systems.

The strategic remediation management action plan should also identify the staff responsible for reporting to senior management on the progress and tracking the improvements to completion.

7.4.6 Sharing with a Wider Audience

The outputs of the exercise can be summarised into a "Lessons Learned" document, redacting details that would otherwise expose sensitive information, that can be shared with other members of the industry or a broader community for the common benefit.

8 Appendix

8.1 Deliverables

This section provides indicative samples of deliverables to be tailored to suit individual FIs, depending on level of services provided and outcomes desired. Headings may vary.

8.1.1 Exercise Preparation Report

The Exercise preparation report is created by the Exercise Working Group during the initial preparation phase. It will contain the details and decisions for the exercise.

Report structure sample

1. Introduction (including The Team composition, the name and the role of each member)
2. Exercise Preparation
2.1 Exercise Description
2.2 Exercise Code Name
3. Attack Execution
3.1 Objectives and Scope
3.1.1 Attack Objectives
3.1.2 Attack Scenarios
4. Communication Management Strategy
4.1 Contacts
4.1.1 Organisation
4.1.2 Attackers
4.2 Email and File Exchange

8.1.2 Threat Modelling Report

The Threat Modelling Report is produced either by the Attacker or by a separate group (may be even a different provider) that specialises in Threat Intelligence. Threat Intelligence analysts will analyse the kinds of threats that are currently prevalent, either non-specific or specific to the FI, and will put this information in a report that is used to create plausible and credible scenarios of attack.

In the Threat Modelling Report, the intent and capability of the threat actors are also assessed and ranked using a threat matrix and summary table. The FI would then use the information in this report to subsequently plan the exercise.

8.1.2.1 Generic Threat Intelligence Report

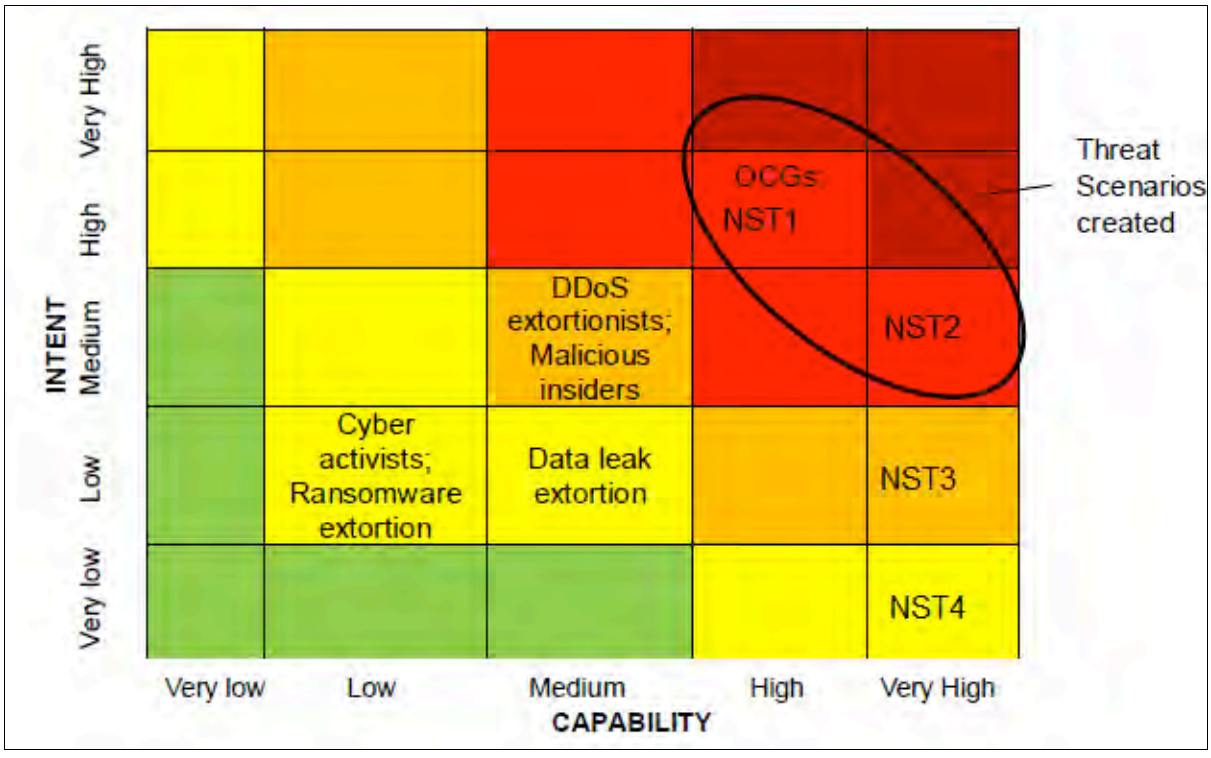
The Threat Modelling Report should contain information on potential real-world attackers' modes of operation and their TTPs. This does not necessarily apply to the FI being targeted, but applies to most organisations in general.

8.1.2.2 Targeted Threat Intelligence Report

The Targeted Threat Modelling report contains information on threats, attackers and TTPs specific to the FI or its industry type. This may include threats that are specific due to a certain geopolitical condition, FI's involvement in certain projects, competitor landscape, etc.

Report structure sample

Threat matrix sample



Threat Summary Table Sample

Threat Actor	Intent	Capability	Threat	Summary
Organised cybercriminal groups (OCGs)	High	High	HIGH	OCGs are the most sophisticated of cybercriminal actors, and have demonstrated their capability to compromise various different types of systems in scope for this engagement. Although they have been more active in financial centres other than Country X, Organisation X will still likely represent an attractive target.
NST1	High	High	HIGH	
NST2	High	Very High	HIGH	
DDoS extortionists	Medium	Medium	MEDIUM	DDoS extortionists have successfully targeted organisations with a similar profile to the organisation in the past, and may look to disrupt the organisation's public-facing web portals to extract ransoms.
Malicious insiders	Medium	Medium	MEDIUM	Malicious insiders' privileged access to key systems and information potentially renders them among the most capable actors in this assessment, though we have uncovered no explicit evidence to suggest that insiders are looking to target Organisation X.
NST1	Low	Very High	MEDIUM	
Ransomware extortion	Low	Low	LOW	Organisation X will likely face a high volume of ransomware extortion activity, though the perpetrators will generally lack the intent or capability to specifically target the in-scope systems.

Data leak extortion	Low	Medium	LOW	Data leak extortionists may have the ability to breach and threaten to release sensitive information from Organisation X key systems, though are more likely to pursue smaller and more vulnerable organisations.
Cyber activists	Low	Low	LOW	With the possible exception of launching DDoS attacks against online banking portals, cyber activists lack the capability required to target Organisation X in-scope systems. This will also deter their intent to do so.
NST2	Very Low	Very High	LOW	

8.1.3 Targeting Report

The Targeting Report prepared by the Attacker contains all the information about the targeted organisation. It will help the Attacker breach the organisation and move closer the objectives by understanding the various controls in place to bypass as well as the overall attack surface.

Report structure sample

Executive Summary
1. Targeting Organisation
1.1 Phishing Campaigns
1.1 Security Controls (Email filtering, File integrity monitoring, Egress restrictions, Office macros, …)
2. Key Systems (Retail banking, Commercial banking, Trading and sales, Payment and settlement, …)
2.1 Key Personnel (Related to the systems identified above)
2.2 Key Suppliers (Related to the systems identified above)
2.3 Technical Details (Related to the systems identified above)
3. Organisation and People
3.1 Organisation Structure
3.2 Organisation Policies (Employee benefits, Whistle blowing campaigns)
3.3 Organisation Announcements (Acquisition, Deployment of large solutions)
3.4 Organisation Awards (Best employers, Safest Bank, ...)
3.5 Organisation Events (Sports related, charity, ...)
3.6 Social Media Presence (Facebook, Twitter, Instagram, LinkedIn, ...)
3.7 Office Locations
3.8 Key Customer, Supervisory and Audit Relationships (MAS, ABS, ...)
3.9 Employees
4. General Networks and Systems

4.1 Autonomous System Numbers (ASN)
4.2 IP Netblocks (IPv4 and IPv6)
4.3 DNS Domain Names
4.4 Registered X.509 Certificates
4.5 Enumerated Hosts
5. Email
5.1 Gateway Infrastructure
5.2 Content
5.3 Address Format
6. General Technologies
6.1 Critical Functions
6.2 Cloud
6.3 Security
6.4 Networking
6.5 Server
6.6 Desktop
6.7 Mobile
6.8 Other
7. Key Suppliers
Appendix I - Reconnaissance Methods

8.1.4 Execution Log Report

An Execution Log Report is a live document that should be maintained by the Attackers throughout the exercise, providing an overview of the exercise and describing the course of actions, proposed future strategies, decisions made, changes in direction and other such reasoning.

The execution log contains information on resources that were utilised to achieve goals and/or scenarios, and highlight the attack path taken by the simulated adversary.

Report structure samples

1. Introduction
2. Project Overview
2.1 Key Functions
2.2 Attack Path
Network foothold, sustained access, action on objectives
Out of scope techniques: Phishing attacks on Organisation's customers, Compromising third party sites as part of a watering hole attack
3. Assessment Plan (for each phase: Status, Objective, Methodology, Outcome, Requirements, Details)
3.1 Reconnaissance
3.2 Staging
3.3 Exploitation
3.4 Control and Movement

3.5 Persistence and Egress
3.6 Attack Execution
4. Concessions and specific Information (for each stage: Reconnaissance, Staging, Exploitation, Control and Movement, Persistence and Egress, Attack Execution)
5. Attack Attribution (Protocol to clarify whether or not an actual unauthorised attacker has gained access to sensitive systems or data, and to prevent unnecessary initiation of expensive incident handling procedures in response. On the other hand, if an attack which is not attributable to the Simulated Attacker (Red Team) is detected, then this provides the opportunity to ask the Legitimate Attacker's team to stand down so as to avoid interfering with or confusing the incident responders.)

8.1.5 Exercise Report

The Exercise Report, also known as the Attackers' Report, is the final report published by the Attackers after the exercise is concluded. It describes the actual scenario-based attack as it played out, listing the attack elements that were critical to the success of the attack, e.g. weaknesses discovered that enabled the Attackers to progress to the next stage. This report is used as the source of information for remediation and clean-up activity planning.

The Exercise Report should also contain recommendations on remediation, both tactical and strategic, based on the Attackers' expertise and experience.

The Exercise Report should contain a timeline containing pertinent information about the attack as it unfolded, which will assist in creating a Defence Report, in order to reconcile the activities of both sides.

Report structure sample

Part 1 - Executive Overview
1.1 Strategic Recommendations
1.2 Security Benchmark
Part 2 - Project Scope and Methodology
Part 3 - Findings
Part 4 - Recommendations
Part 3 - Prevention
Part 4 - Detection & Response
Part 5 - Attack Details
5.0 Threat Intelligence and Modelling
5.1 Reconnaissance
5.2 Phishing
5.3 Local Privilege Escalation
5.4 Information Gathering
5.5 Use of concessions and deviation from live environment
5.6 Lateral Movement
5.7 Researching Attack Objectives

8.1.6 Clean-up Report

A Clean-up Report should be prepared by the FI as soon as the attack report is published. It should detail IOCs and artefacts on any residual data or changes made during the exercise, for removal by an internal system administrator team. Internal parties are typically best placed to execute a clean-up, due to knowledge of internal processes, legitimate credentials and access held and knowledge of controls or intricacies that a simulated Attacker may not have visibility of.

8.1.7 Defence Report

A Defence Report, or a Blue Team report, should be prepared by the defence teams based on the Exercise Report, in order to reconcile the attack timeline from the defenders' point of view. It should describe at which stages and at which points the Attackers were uncovered (if any), or their artefacts encountered.

8.1.8 Remediation Management Action Plan

A Remediation Management Action Plan should be produced by the FI, assisted by recommendations from the Exercise Report, but also information from its own internal risk assessment. This report should outline the identified systemic vulnerabilities and gaps through the course of the exercise, and the Management's committed activities in order to remediate them. A project manager should be assigned to track these actions to closure, with periodic reporting to the Sponsoring Executive or senior management.

9 References

9.1 Relevant Frameworks

CBEST:

- https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity
- CBEST implementation guide
- CBEST services assessment guide
- Understanding cyber threat intelligence operations
- Cyber resilience questionnaire

TIBER-NL :

- https://www.dnb.nl/en/news/news-and-archive/nieuws-2017/dnb365801.jsp
- https://www.dnb.nl/en/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm47-365455.pdf

TIBER-EU:

- https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html
  https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

iCAST, part of C-RAF:

- http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf
- http://www.cyberworld.com.hk/wp-content/uploads/custom/eDM/17Q3CW/CRAFreport.pdf

9.2 Additional references

ATT&CK (Adversarial Tactics, Techniques & Common Knowledge):

- https://attack.mitre.org/wiki/Main_Page

10 Glossary

ABS	Association of Banks in Singapore
AIM	Access and Identity Management
BAU	Business-As-Usual
BT	Blue Team
C2, C&C	Command and Control infrastructure
CBEST	Cyber resilience program – Bank of England

CF	Critical Function
CISO	Chief Information Security Officer
C-RAF	Cyber Resilience Assessment Framework – HKMA in HK
DNS	Domain Name Service
iCAST	Intelligence-led Cyber Attack Simulation Testing
IT	Information Technology
RT	Red Team
SCCS	Standing Committee for Cyber Security
TIBER	Threat Intelligence Based Ethical Red-teaming – DNB in NL or ECB in EU
TTP	Tactics, Techniques and Procedures used by attackers

11 Acknowledgements

- ABS Standing Commitutee on Cyber Secrity (SCCS)
  - Chairmanship: Standard Chartered Bank

- SCCS Working Group (AASE)
  - Project Lead: DBS Bank Ltd
  - Members

    - BAML
    - CSA
    - Citibank
    - Credit Suisse
    - Deutsche Bank
    - HSBC
    - JP Morgan Chase
    - MAS
    - Maybank
    - OCBC
    - Standard Chartered Bank