Cyber Operational Resilience Intelligence-led Exercises (CORIE)® Framework

Program Guide

for Financial Institutions (including Financial Market Infrastructure) in Australia

Version 2.0

July 2022

Council of Financial Regulators

Contents

Glossary

Term	Explanation
Adversary Attack Simulation	An exercise that uses Threat Intelligence to model and execute an adversary attack simulation. Also known as a Red Team Exercise.
APRA	Australian Prudential Regulation Authority.
ASIC	Australian Securities and Investments Commission.
Blue Team	The FI's team tasked to defend against adversaries attacking their organisation.
CFR	Council of Financial Regulators.
Control Group (formerly White Team)	The FI's team tasked to oversee an Exercise.
CORIE	Cyber Operational Resilience Intelligence-led Exercises.
CTC	CORIE Team Coordinators – tasked with the day-to-day management of the program in accordance with this guide. The CTC includes representative members from the CFR.
Exercise	A cyber operational resilience intelligence-led exercise, likely to consist of an adversary attack simulation, e.g., Red Team Exercise.
FI	A financial institution (including an entity responsible for financial market infrastructure) that participates in the program.
Gold Team Exercise	A Table Top exercise that involves the Provider performing crisis simulations. The exercise involves the FI's senior executives (Gold Team) or crisis management team. The exercise is also known as a Table Top Crisis Simulation.
Modus Operandi	A manner or mode of operating or working.
OSINT	Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources.
Participant	A financial institution (including an entity responsible for financial market infrastructure) that participates in the program.
Provider	A third-party that an FI engages to perform an Exercise. Recognised Providers are identified by having met minimum requirements.
PID	Project Initiation Document.
PIM	Project Initiation Meeting.
Purple Exercise	An exercise that involves the Red Team replaying attacks to help the Blue Team identify gaps to remediate. Also known as a Replay Adversary Attack Simulation.
RBA	Reserve Bank of Australia.
Red Team	The Provider team tasked to simulate an adversary attacking the FI.
Red Team Exercise	An exercise that uses Threat Intelligence to model and execute an adversary attack simulation. Also known as an Adversary Attack Simulation.
Regulator	One or more of APRA, ASIC, and the RBA.

Replay Adversary Attack Simulation	An exercise that involves the Red Team replaying attacks to help the Blue Team identify gaps to remediate. Also known as a Purple Exercise.
Table Top Crisis Simulation	A Table Top exercise involving the Provider performing crisis simulations. The exercise involves the FI's senior executives (Gold Team) or crisis management team. The exercise is also known as a Gold Team Exercise.
Threat Intelligence	Threat intelligence[1] is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

1 https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

Background

Cyber risk is repeatedly classified amongst the top risks to the Australian financial system and is a key risk on the Council of Financial Regulators (CFR) risk register[2].

In March 2019, the CFR Cyber Security Working Group (Cyber WG) proposed establishing a framework for improving cyber resilience within the Australian financial services industry[3]. The proposal's intent was to create a framework using targeted threat intelligence to build goal-focused 'red team' scenarios that test and demonstrate an institutions' cyber resilience level. Similar schemes have been formed by central banks in overseas jurisdictions and continue to assess maturity against cyber-attack trends rising in frequency and sophistication[4].

Red team exercises mimic the tactics, techniques, and procedures (TTP's) of real-life adversaries, employing creativity and utilising tools and techniques that may not have been anticipated and planned for. These exercises measure the ability of an organisation to detect, respond, withstand, repel, and recover from the operations of a real adversary based on such TTPs, to maintain critical business processes and protect sensitive data.

The Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework has been developed by the CFR, to aid in preparation and execution of industry-wide cyber resilience exercises. A pilot program was completed in 2021 to test the framework with the participation of multiple financial institutions.

2 The role of the CFR is to contribute to the efficiency and effectiveness of financial regulation and to promote the stability of the Australian financial system. Membership of the CFR consists of the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), the Reserve Bank of Australia (RBA), the Department of Treasury. https://www.cfr.gov.au/financial-stability/cyber-security.html

3 In addition to CFR agencies, the Cyber WG includes the Department of Home Affairs (Home Affairs) which is responsible for developing and coordinating the national approach to cyber security. Home Affairs includes a Cyber Security Policy Division embedded within the Australian Cyber Security Centre (an Australian Signals Directorate (ASD) organisation), which brings together technical capabilities from across the Australian Government into a single location.

4 Similar schemes include CBEST, Threat Intelligence Based Ethical Red-teaming (TIBER), intelligence-led Cyber Attack Simulation (iCAST), and the Adversarial Attack Simulation Exercise (AASE).

1. Introduction

Sophisticated adversaries are continuously attacking Australian Financial Institutions (FIs) in illegal operations that can result in substantial financial loss, reputational damage, and in a worst-case scenario impact the stability of the Australian financial markets and financial system.

Cyber operational resilience requires that people, processes, and information systems adapt to the ever-evolving threat landscape. To maintain the ability of financial institutions to avoid significant financial loss and worst-case scenarios, cyber operational resilience must be proactive and not reactive.

As outlined in this guide, CORIE is a program of exercises aiming to assess a financial institution's cyber resilience. These exercises use intelligence gathered on adversaries, to simulate their modes of operation. Threat intelligence-led exercises aim to assess the overall maturity of a financial institution's cyber defence and response capability.

Real-life adversaries such as state-sponsored attackers are neither constrained by scope nor time. CORIE exercises mimic adversaries through fewer traditional testing restrictions and longer time duration to fully exploit opportunities. As a result, CORIE complements traditional security testing programs, such as vulnerability assessments, penetration testing and continuous red teaming – financial institutions should continue to maintain their existing security testing regimes.

Exercises will be conducted by independent Providers, bringing a fresh perspective, and as close to an unbiased view as possible coupled with advanced adversary simulation capabilities. Day-to-day management of the program is performed on behalf of the CFR by the CORIE Team Coordinators (CTC), consisting of a small number of trusted personnel within the cyber security teams of the CFR members.

On completion of exercises, a report detailing industry-wide cyber resilience trends amongst FIs will be presented to the CFR highlighting any systemic weaknesses that may present a risk to the integrity of the Australian financial markets and financial system.

CORIE should not be seen as a pass/fail exercise, or as a tool for benchmarking FIs.

This guide is intended to provide the framework necessary for the CTC, FIs, and Providers to participate in the CORIE program.

1.1 Objectives of the CORIE program

The program will focus on the following objectives:

- Provide data and information to inform relevant Australian Regulators[5] of systemic weaknesses that may present a risk to the integrity of the Australian financial markets and financial system
- Assess FI's resilience to known adversaries targeting the FI
- Provide the relevant Regulator and FI with a plan of remediation to address any identified weaknesses.

1.1.1 Threat Intelligence

Threat Intelligence should:

- Identify primary adversaries targeting the FI
- Identify adversaries' modus operandi
- Gather available information that will aid in the success of the modus operandi
- Provide the FI with an understanding of the information available about them.

5 Regulators include Australian Prudential Regulation Authority (APRA), Australian Securities Investments Commission (ASIC), and Reserve Bank of Australia (RBA)

1.1.2 Adversary Attack Simulation (Red Team Exercise)

A Red Team exercise should:

- Assess people, processes, and technology end-to-end maturity with regards to cyber defence not otherwise assessed by traditional vulnerability assessment and security testing methodologies
- Assess the FI's security prevention, detection, and response capability
- Reveal attack paths and techniques that may have not been considered
- Assess the maturity of the FI's processes in reacting to adversaries.

1.1.3 Replay Adversary Attack Simulation (Purple Exercise)

A Replay Adversary Attack Simulation should:

- Systematically replay simulated adversary tactics, techniques, and procedures to ensure the FI's defences are improved
- Exchange knowledge between the offensive and defensive teams.

1.1.4 Table Top Crisis Simulation (Gold Team Exercise)

A Table Top Crisis Simulation should:

- Assess the FI's Executives on security incident management and/or crisis management response and processes.

1.2 Resource Overview

Only Red Team exercises require an external provider.

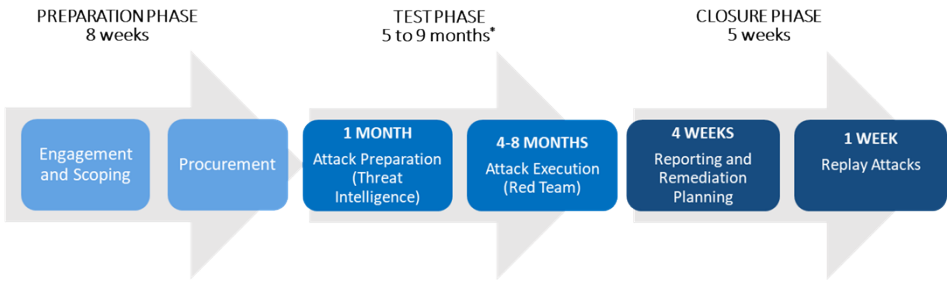
Purple and Gold exercises can be performed with internal resources if preferred.

Figure 1 - External and internal resources

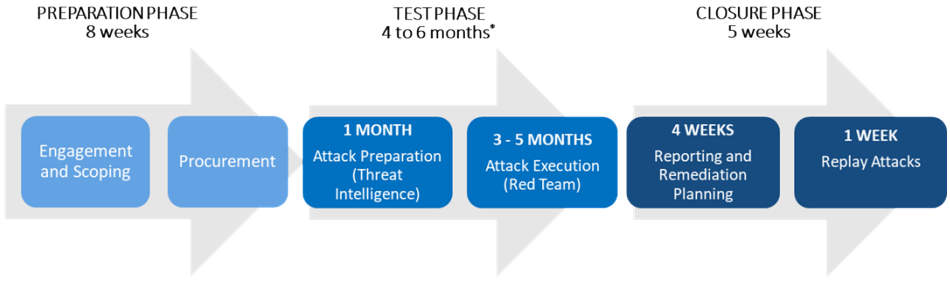
1.3 Adversary Attack Simulation Timeframe Overview

Suggested timeframes for phases within the Adversary Attack Simulation (Red Team) exercise are intended to constrain costs and effort. This is dependent on the number of scenarios and selected CBS.

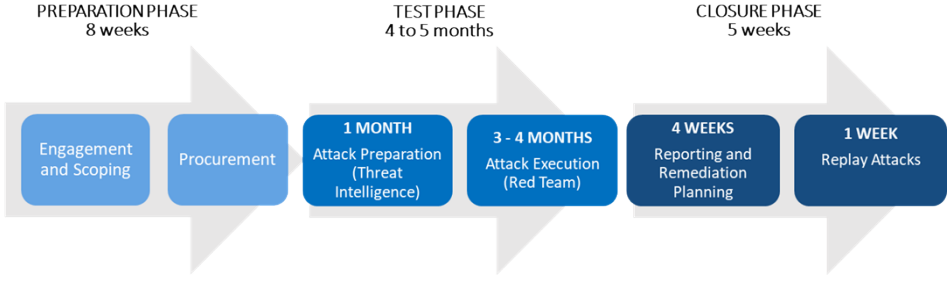
3 Scenario Calendar Duration



2 Scenario Calendar Duration



1 Scenario Calendar Duration



* Where TI is 1 month and an FI may choose to execute scenarios in parallel or stop attack execution in various situations, eg real incident.

Figure 2 - Phases and timeline within a Threat Intelligence-led Adversary Attack Simulation (Red Team) exercise

2. Governance and Management

The members of the CFR leading CORIE's management and governance will continuously improve the CORIE scheme using feedback and lessons learned from each exercise.

2.1 Roles and Responsibilities

The relevant Regulator will assess the risk an FI poses to the stability of the Australian financial markets and financial system, and will propose the following in a structured and defined way:

- Type and details of the exercise
- Frequency of the exercise
- How threat intelligence is gathered and used within the exercise.

The CTC will manage Exercises on behalf of the CFR with a view to ensuring they are:

- Conducted by a Provider that meets specified minimum standards
- Executed as close as possible to the modelled intelligence-led scenarios
- Completed with cooperation and without unfair obstruction from the FI.

The relevant Regulator and CTC will review the outcome of the exercise to:

- Ensure it has been conducted in accordance with this CORIE guide
- Gain knowledge of any weaknesses that may impact the stability of the Australian financial markets and financial system
- Track the remediation of any important weaknesses identified
- Identify systemic weaknesses across the FIs
- Determine whether further exercises would be appropriate in relation to the FI.

2.2 Providers

Providers that wish to participate in the program should meet specified minimum standards.

Providers with a significant presence in Australia are preferred due to ease of use when co-ordinating effort.

A Provider may participate in the program as a Threat Intelligence Provider and/or a Red Team Provider.

2.3 Threat Intelligence Provider

A Threat Intelligence Provider gathers threat Intelligence on adversaries targeting FIs in Australia.

Other sources of intelligence used in the program may include:

- Government
- Internal FI sources
- Proprietary feeds
- Intelligence sharing platforms
- Generic public threat intelligence.

A Threat Intelligence Provider engaged by an FI must satisfy the FI that it has a mechanism to gather information and develop threat intelligence from the dark web and that all threat intelligence will be gathered in a legal and ethical manner.

FIs should satisfy themselves that the Threat Intelligence Provider they engage has certified resources to threat model and perform analysis on real-world threats that appear, or are known, to be targeting the FI.

FIs should satisfy themselves that the Threat Intelligence Provider they engage has appropriately certified resources and demonstrable experience to provide both a Threat Intelligence Report and Targeting Report to both the FI and CFR.

2.3.1 Threat Intelligence Team Member Requirements

FIs should satisfy themselves that the personnel of the Threat Intelligence Provider they engage meet the requirements set out in this section 2.3.

A Threat Intelligence team should have qualified and experienced consultants capable of performing analysis, threat modelling and reporting at the time of the engagement.

The team should consist of at least one Threat Intelligence Lead and one Threat Intelligence Analyst.

2.3.1.1 Threat Intelligence Lead

A Threat Intelligence Lead is expected to have knowledge and expertise in leading a team specialising in producing threat intelligence. They should have the ability to gather threat intelligence in a realistic, legal, and safe manner with the ability to document appropriate supporting evidence.

2.3.1.2 Threat Intelligence Analyst

Threat Intelligence Analysts are expected to have knowledge and expertise to gather threat intelligence in a realistic, legal, and safe manner, collecting appropriate supporting evidence.

2.3.1.3 Threat Intelligence Skills Matrix

The criteria resources should meet to execute any of the CORIE exercises is covered in 14.2 Appendix B: Provider Guide.

2.4 Provider for Adversary Attack Simulation – Red Team Exercise

FIs should satisfy themselves that the personnel of the Red Team Provider they engage meet the requirements set out in this section 2.4.

Red Team Providers should have qualified and experienced team members capable of performing management, OSINT, reconnaissance, surveillance, cyber-attack simulation, social engineering, physical breach, and reporting at the time of the engagement.

A Red Team should consist of at least a Red Team Lead, a Red Team Specialist, and an Exploit Development Specialist.

2.4.1 Red Team Member Requirements

2.4.1.1 Red Team Lead

Red Team Leads are expected to have strong practical and theoretical knowledge and expertise in simulating sophisticated adversaries targeting organisations within the financial industry, along with expertise in leading a Red Team. The Red Team Lead should have skills to create schedules, test plans, action summaries, and run meetings and workshops with the FI. Red Team Leads should be proficient in identifying, managing, and communicating exercise risks to the FI's Control Group. They should also provide practical advice and solutions to resolve challenges that typically arise during engagements.

2.4.1.2 Red Team Specialist

Red Team Specialists are expected to have practical knowledge and expertise in simulating sophisticated adversaries targeting organisations within the financial industry. They should have skills encompassing

exploitation of vulnerabilities, social engineering phishing campaigns, implant development, evasion skills and lateral movement within a compromised network.

2.4.1.3 Exploit Development Specialist

Exploit Development Specialists are expected to have experience developing software exploits and improving public exploits for use in production environments. The Exploit Development Specialist should have skills around exploit development, reverse engineering, assembly, and disassembly, along with a comprehensive knowledge of different operating systems and their defences.

Exploit Development Specialists are not expected to be engaged in the exercise on a full-time basis, but should be available to create, modify, and improve exploits for the exercise when required.

2.4.1.4 Red Team Member

Red Team Members are expected to have knowledge and expertise in simulating adversaries targeting organisations in the financial sector. They should have skills to support the Red Team Specialist and execute specific tasks assigned to them. Due to the increased scope of larger exercises, Red Team Members provide support for tasks requiring less complexity. Red Team Members should not work on the exercise without a Red Team Specialist. Actions on targets are the responsibility of the Red Team Lead and Red Team Specialist, including those of the Red Team Member.

2.4.1.5 Red Team Skills Matrix

The criteria resources should meet to execute any of the CORIE exercises is covered in 14.2 Appendix B: Provider Guide.

2.5 Provider for Replay Adversary Attack Simulation – Purple Exercise

A Purple Exercise should be completed by Tier 1, 2 and 3 FIs annually.

Purple Exercises originate from the concept of the Red Team and Blue Team intermixing. The Red Team, who simulate attacks, collaborates with the Blue Team, which is the team responsible for detecting and responding to cyber-attacks in an organisation.

Where an FI has an internal testing capability that meets the requirements of this section, the internal team can be used to conduct this exercise rather than using an external Red Team Provider. The internal team then becomes known as the Provider for all intents and purposes.

Figure 3 - External and internal resources

Providers must have qualified team members to mimic the tactics, techniques, and procedures of known advanced persistent threats.

The Provider's Red Team will work closely with the FI's Blue Team.

2.5.1 Purple Exercise Member Requirements

Purple Exercises can be conducted by the following Red Team Provider members:

- Red Team Specialist
- Red Team Member

2.6 Provider for Crisis Simulation Table Top – Gold Team Exercise

A Gold Team Exercise should be completed by Tier 1, 2 and 3 FIs annually.

Providers should have qualified team members that can clearly communicate, and have knowledge concerning details of scenarios involved adversary attack simulation. Team members must have knowledge of the appropriate defensive counter measures and risk management used within FIs.

As the skills required match many of those required by the Red Team Provider to lead an adversary attack simulation, a Red Team Provider can be used for a Gold Team Exercise.

Consistent with approach to Purple Exercises, where an FI has an internal testing capability that meets the requirements of this section, the internal team can be used to conduct this exercise rather than using an external Red Team Provider.

That team then becomes known as the Provider for all intents and purposes.

Figure 4 - External and internal resources

2.6.1 Gold Team Member Requirements

2.6.1.1 Gold Team Lead

Executives may have little prior awareness or exposure to the concepts, terms or details of adversary attack simulation, therefore Gold Team Leads should have strong communication and facilitation skills to lead in role playing activities simulating diverse crisis events.

Gold Team Leads should understand risk management, along with possessing strong practical and theoretical knowledge in simulating sophisticated adversaries, and defensive capabilities used to prevent, detect, and respond accordingly. Further, Gold Team Leads must be able to convey risks in terms of business impact and likelihood, so that executive management understand appropriate actions to undertake.

Provider staff with skills necessary to lead a Gold Team can be assigned the role of Gold Team Lead. However, either a Red Team Lead or Red Team Specialist should also be a member of the Provider's team.

3. Cyber Risk Assessment

The Cyber Risk Assessment (CRA) is an assessment tool to evaluate and categorise FI's according to the level of risk their compromise poses to the stability of the Australia financial markets and financial system, against a high-level view of their cyber resilience. The assessment will determine exercise types and frequency.

3.1 Cyber Risk Questionnaire Assessment

Each FI will receive a CRA questionnaire from the CTC for completion and return to the CTC prior to the commencement of the program.

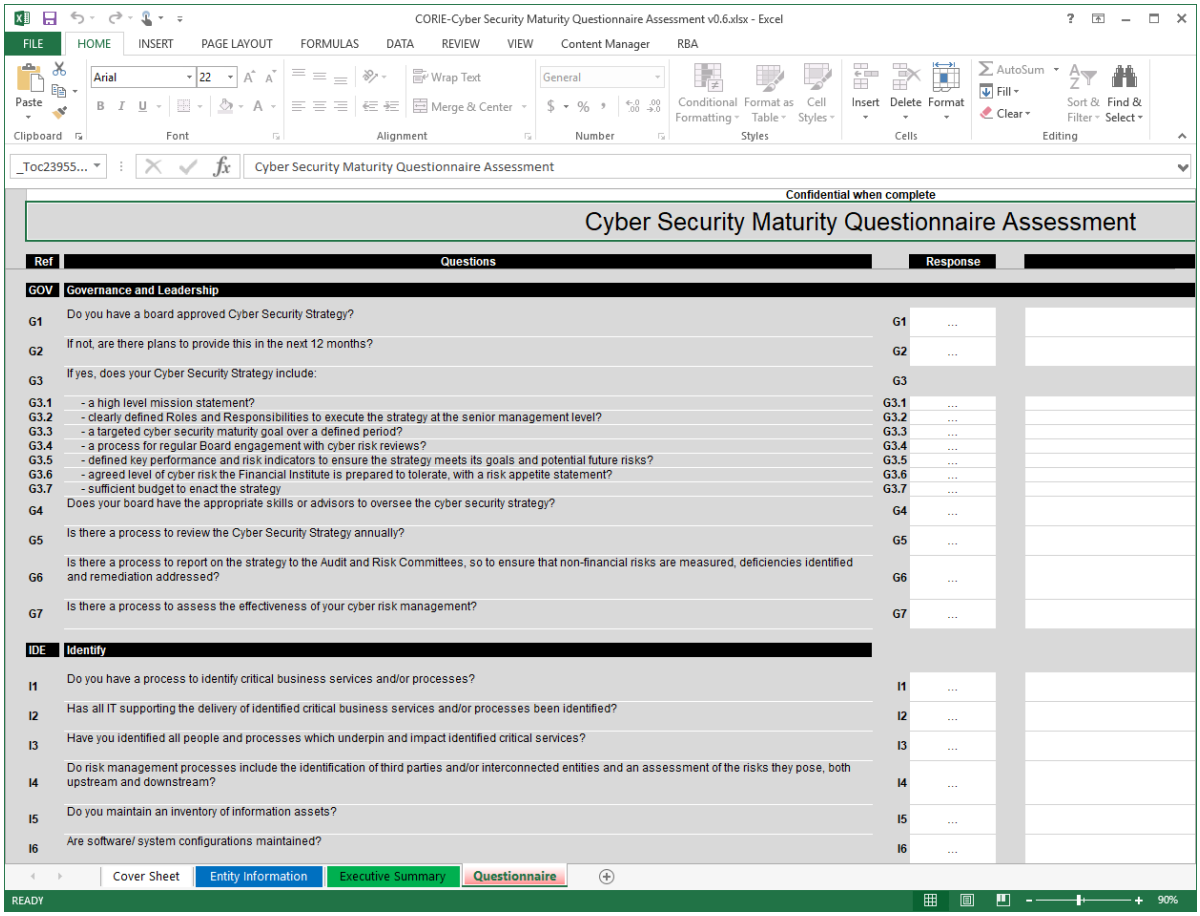


Figure 5 – An example image of the CRA Questionnaire

4. The CORIE Scheme

4.1 Industry Pilot Program

An industry pilot of CORIE was completed in 2021. The pilot consisted of a small number of systemically important FIs invited by the CFR to participate and provide feedback.

Workshops were conducted to gather feedback from Providers and FI participants and has been used to update the framework as part of its implementation into industry.

4.2 Implementation

In implementation, CORIE involves an invitation of participation sent to FIs. Each time the CFR will invite a new group of FI to participate.

For completeness, implementation may require FIs to complete the CRA before the frequency and type of exercises is individually defined. If required, this will be made known at the time of invitation.

After exercise types are defined, the FI should use this guide to complete the requirements of the exercise.

Previous participants should use the additional exercises in this guide as a baseline until required to repeat the primary exercise, Adversary Attack Simulation.

4.3 Market Risk Assessment

A Market Risk Assessment (MRA) will categorise the FI by the level of risk their compromise poses to the stability of the Australian financial markets and financial system. This will be based on parameters like market capitalisation, total assets, and FIs deemed systemically important by the CFR.

The MRA is determined by the CFR – there are no actions for FI's or Providers.

4.4 CTC Communication and Engagement

4.4.1 Provider Assessment

The CTC will assess whether Providers meet the specified minimum standards referred to in section 2. Those that do not meet the standards in section 2 should not provide services for the CORIE program. For efficiency, FIs should confirm their top three most preferred CORIE Providers with the CTC before finalising their procurement process – this may save some time and effort.

4.4.2 Exercise Involvement

The CTC will be involved at defined points throughout the program. Those points of involvement are set out in this guide.

Any queries around CTC involvement should be made via the CTC mailbox detailed in Annex A: CTC Contact Details.

4.4.3 Issues Resolution

Should issues arise between an exercise Provider and FI that would impact the integrity or results of the exercise, these issues, if not able to be resolved promptly between the FI and the Provider, should be escalated to the CTC for comment. The CTC may liaise with CFR members in relation to matters referred to it for comment.

Issues may include:

- Unreasonable challenges or obstructions preventing the Provider from simulating a scenario
- Provider team members unavailable during an exercise without a contingency plan

- Any malicious actions that might impact the FI during the course of the exercise.

Requests for CTC comment on relevant issues should be sent via the CTC mailbox detailed in Annex A: CTC Contact Details.

4.4.4 Report Sharing

Specific to the Adversary Attack Simulation – Red Team Exercise, the CTC will receive FI and Provider reports during the course of an exercise. These reports may be used by CFR to determine a consistent view of industry participants and balance out any irregularities during exercises. For example, one Provider may rate a test outcome as low risk, versus another Provider rating the same outcome as high risk – in this instance the CTC will contact the affected Provider and FI on behalf of the CFR to promote a consistent outcome of the exercise. Raw reports will also be compared against risk managed reports to help identify industry trends.

Reports are to be sent at the defined points detailed in this guide.

Providers and FIs can contact the CTC to receive instructions on how to securely share reports with the CFR via CTC.

The CTC mailbox is detailed in Annex A: CTC Contact Details.

4.5 Data Management

Providers and FIs that share and access sensitive exercise data and reports should manage the data in line with security best practices.

For Providers, procedures around sharing sensitive exercise data should assure the FI and CFR that the data is secured in transit, and at rest.

Sensitive exercise artefacts are recommended to be securely destroyed by Providers at completion of the exercise, bearing in mind that exercise reports or artefacts may be beneficial to complete further exercises e.g., Replay Attacks. The CTC will securely destroy participant data and reports at the end of each exercise cycle.

FI's are responsible for advising Providers of an acceptable data retention period, and any data destruction requirements. These requirements are recommended to be contractual obligations between the FI and their Providers.

5. Threat Intelligence-led Adversary Attack Simulation – Red Team Exercise

5.1 Summary

The Threat Intelligence-led Adversary Attack Simulation (Red Team exercise) will test and assess the FI's cyber resilience to attacks mimicking specific methods of identified adversaries. These exercises will be conducted by a Provider that brings a fresh perspective and as close to an unbiased view as possible, in order for an independent assessment to be achieved.

Collecting Threat Intelligence helps FIs identify their adversaries together with related tactics, techniques, and procedures used to target specific business services. With this information, the Red Team Provider can simulate real life attack scenarios against FI's people, process and production infrastructure to assess and improve cyber resilience.

The adversary simulation should be performed as close as possible to real life scenarios as feasible, also aligning to the FI's risk appetite when testing against in-scope production services.

Efficacy of adversary simulations is improved when the FI's defensive teams have no knowledge of the exercise before and during delivery.

Importantly, one of the primary outcomes of the simulation is an uplift in the FI's awareness by identifying potential gaps and actions to improve their defences. This is delivered through a detailed post exercise debrief between the Red Team and FI's defensive teams.

The Red Team exercise consists of six (6) stages performed across three (3) phases:

1. Preparation Phase
    - Stage 1: Engagement and Scoping
    - Stage 2: Procurement
2. Test Phase
    - Stage 3: Attack Preparation – Threat Intelligence
    - Stage 4: Attack Execution – Red Team
3. Closure Phase
    - Stage 5: Reporting and Remediation Planning
    - Stage 6: Replay Attacks

The Preparation Phase consists of engagement with different parties participating in the CORIE scheme, identification of critical business services, scoping the engagement, and the procurement process to identify and contract Provider(s).

The Test Phase comprises Attack Preparation and Attack Execution stages. Attack Preparation entails acquisition of Threat Intelligence to shape scenarios in the Attack Execution stage.

The Closure Phase includes the Red Team finalising and presenting reports to the CTC/CFR, relevant Regulator, Blue Team, FI's Control Group, and other key stakeholders in debrief meetings. The Red Team will also replay specific attacks identified as a defensive weakness.

To complete the Closure Phase, the FI details a remediation plan and provides an outline to the CFR via the CTC.

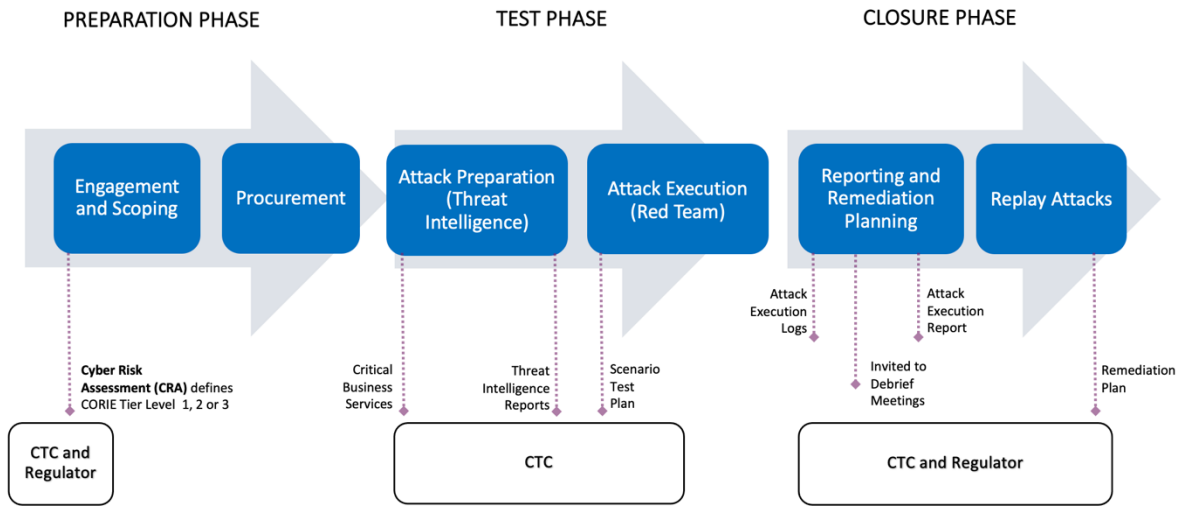


Figure 6 - The Threat Intelligence-led Adversary Attack Simulation is split into three phases (Preparation, Test, and Closure) over multiple months.

5.2 Red Team Exercise Scenario Examples

5.2.1 Example Scenario 1

5.2.1.1 Identifying Critical Business Services

The FI and CTC have agreed on Critical Business Services (CBS):

- Payment System 1 (PS1)

(CBS are explained in section 5.5 Critical Business Services and Scenarios)

5.2.1.2 Threat Intelligence

Threat Intelligence has identified an adversary, Nation State 1 (NS1), targeting regional FI's PS1 to initiate fraudulent payment transactions.

NS1's known modes of operation include:

- Initial Access – social engineering, including spear phishing attachments and watering hole techniques
- Execution – client execution through exploitation of vulnerable client software, and circumventing application allow/deny list techniques e.g., reflective DLL injection
- Persistence and C2 – using shortcuts in startup folders, utilising less commonly used, and multiple channels for C2
- Privilege Escalation and Lateral Movement – common Windows privilege escalation techniques, bespoke malware to gain credential access and help achieve lateral movement
- Defence Evasion – multiple techniques to obfuscate network traffic, conceal bespoke payloads, and stopping services to render content inaccessible to users
- Impact – credential and host access leading to fraudulent PS1 payment transactions.

5.2.1.3 Red Team Scenario

Target Scope of Evaluation	Example Approach
Susceptibility to External Breach Perimeter Defences Internal Network CBS: Payment System	Scenario simulates phishing attacks aimed at the FI's staff and their workstations on the internal network, attempts to gain internal network access and compromise PS1's people, process and systems to initiate payment transactions. Attacks involve phishing, spear phishing and watering hole techniques against key PS1 staff members. Simulates the adversary using a custom payload; potentially a bespoke exploit similar to CVE-2017-8572 for credential access and CVE-2018-4878 for client execution. Execution and persistence on the corporate network is a jump off point for further actions on PS1's people, processes and information systems. Simulate a fraudulent PS1 transaction.

	Proposed scenario Flags:
	• Targets derived from Threat Intelligence and OSINT
	• Phishing and or spear phishing PS1's members of staff
	• Persistence and C2
	• Privilege escalation and lateral movement
	  o Workstations and Servers
	  o Active Directory (corporate and PS1 domains)
	  o Databases (PS1 related)
	• Actions on Target
	  o PS1 – simulate fraudulent PS1 transaction
	If a Flag is not achieved, for example compromise of members of staff, a Concession may include nomination of an account to execute a phishing payload, or an account for the Red Team to use to perform the click.

5.2.2 Example Scenario 2

5.2.2.1 Identifying Critical Business Services

The FI and CTC have agreed on CBS:

- Critical and Sensitive Servers

5.2.2.2 Threat Intelligence

Threat Intelligence has identified a local adversary, Organised Crime 1 (OC1), targeting FIs known to have cyber insurance policies. OC1 has been observed using a wide range of attack vectors, including physical attacks, to gain corporate network access.

After initial access, the adversary manually deploys data encryption malware (ransomware) on business-critical servers and related data. Ransoms demand cryptocurrency payment to prevent published breach data and to decrypt files.

OC1 is known to spend months in the corporate network to ensure once data encryption malware is executed in the environment, backups and other business continuity plans are ineffective.

OC1's known modes of operation include:

- Initial Access – phishing campaigns and physical proximity attacks, e.g., malicious media drops and wireless attacks
- Execution – client execution through exploitation of vulnerable client software and leveraged code-signing certificates to sign malware
- Persistence and C2 – deployed rootkits on Windows systems to hide malware and maintain persistence. Using DNS for C2 communications
- Privilege Escalation and Lateral Movement – Windows Credential Editor to dump password hashes from memory and authenticate to other user accounts. RDP commonly used for lateral movement
- Defence Evasion – clearing Windows security and system events, deleted files from systems and use of domain generation algorithms to change C2 servers regularly
- Impact – used a custom ransomware to encrypt files on the targeted systems and provide ransom note
- Exfiltration of breach

5.2.2.3 Red Team Scenario

Target Scope of Evaluation	Example Approach
Physical Proximity Attacks	Scenario simulates close physical proximity attacks on FI's offices and staff, attempts to gain corporate network access to deploy ransomware.
Malicious Media Drop, and or, Wireless Attacks	Attacks target 802.11 wireless networks and staff using wireless peripherals, with opportunistic attacks to deploy malicious media and social engineer staff to connect media to FI's devices.
Internal Network	Execution and persistence on the corporate network is a jump off point for further actions on corporate infrastructure and backup systems.
CBS: Critical and sensitive servers	Simulates control over the corporate network, defined critical and sensitive servers, and related backup solutions.

	Proposed scenario Flags:
	• Targets derived from Threat Intelligence, OSINT, and physical reconnaissance
	• 802.11 wireless attacks
	• Wireless peripherals attacks
	• Opportunistic malicious media drops and social engineering
	• Persistence and C2
	• Privilege escalation and lateral movement
	  ○ Workstations
	  ○ Servers
	• Actions on Target
	  ○ Active Directory (corporate)
	  ○ Binary deployment solutions (e.g., SCCM)
	  ○ Critical and sensitive servers
	  ○ Backup solutions
	If a Flag is not achieved, for example wireless compromise, then corporate wireless credentials or a corporate laptop with corporate network access will be requested in the form of a Concession.

5.2.3 Example Scenario 3

5.2.3.1 Identifying Critical Business Services

The FI and CTC have agreed on the CBS:

- Payment System 2 (PS2)

5.2.3.2 Threat Intelligence

Threat Intelligence has identified an adversary, Organised Crime 2 (OC2), in country X. The adversary is financially motivated and primarily targets FI's. The adversary has targeted components of PS2, successfully exfiltrating card holder data. PS2 payment initiation attempts have also been attributed to OC2.

Evidence from dark web forum posts in their local language show they have also conducted physical attacks in country X, often stealing travellers' devices.

The FI has public offices in their country of operation (country X) with back-office support locally. The likelihood that OC2 will target FI's members of staff travelling for work is high.

OC2 have a high level of capability and intent to steal and use FI's devices to pivot into FI's network and further target PS2.

5.2.3.3 Red Team Scenario

Target Scope of Evaluation	**Example Approach**

Stolen Devices
 	
Insider Threat
 	
CBS: PS2
 	
Exfiltration of valuable (PS2) payment data
	Scenario simulates a stolen corporate laptop and corporate managed phone, attempts to gain internal network access, compromise and exfiltrate valuable (PS2) payment data.
	
	Simulation commences from the perspective of completely powered off laptop with Full Disk Encryption (FDE) through to being left unattended while connected to the corporate VPN.
	
	The latter will also simulate the threats posed by a malicious insider.
	
	Corporate VPN access used to further actions on PS2's people, processes, and information systems.
	
	Simulate compromise and exfiltrate valuable (PS2) payment data.
	
	Proposed scenario Flags:
	
	• Bypass/authenticate against FDE solution
	• Obtain login access to Windows
	• Connect to corporate VPN
	• Privilege escalation and lateral movement
	  ○ Workstations and Servers
	  ○ Active Directory (corporate and PS2 domains)
	  ○ Databases (PS2 related)
	• Actions on Target
	  ○ PS2 application or database compromise to enumerate payment data
	  ○ Exfiltration of valuable (or replica PS2) payment data
	If a Flag is not achieved, for example bypass the FDE solution, then credentials will be requested in the form of a Concession.

5.3 Teams

5.3.1 Control Group

FI's need to assemble a small group of staff, referred to as the Control Group, to oversee the attack simulation and resolve any challenges that arise throughout the exercise.

The Control Group should be limited to senior members of the FI that have appropriate responsibility to make informative risk-based decisions. Those decisions will help ensure the exercise is performed in a safe, controlled manner, balanced with simulating a real-life adversary in a production environment.

Members of the Control Group should be familiar with this guide, have a path of communication to the CTC, and understand the impact of any decision.

The Control Group requires visibility of all Blue Team escalations of attack activity in order to ensure:

- Secrecy and integrity is maintained
- Legitimate attack activity is being properly responded to
- The Red Team are following the scope of the exercise
- Visibility of any Red Team activity detection

The Control Group should provide pragmatic instructions to relevant members of staff if the Red Team is detected.

The Control Group will, when requested, provide timely assistance to the Red Team.

5.3.1.1 Control Group Communication Flow

The following communication flow details all expected interactions in line with the CORIE Adversary Attack Simulation (Red Team exercise).

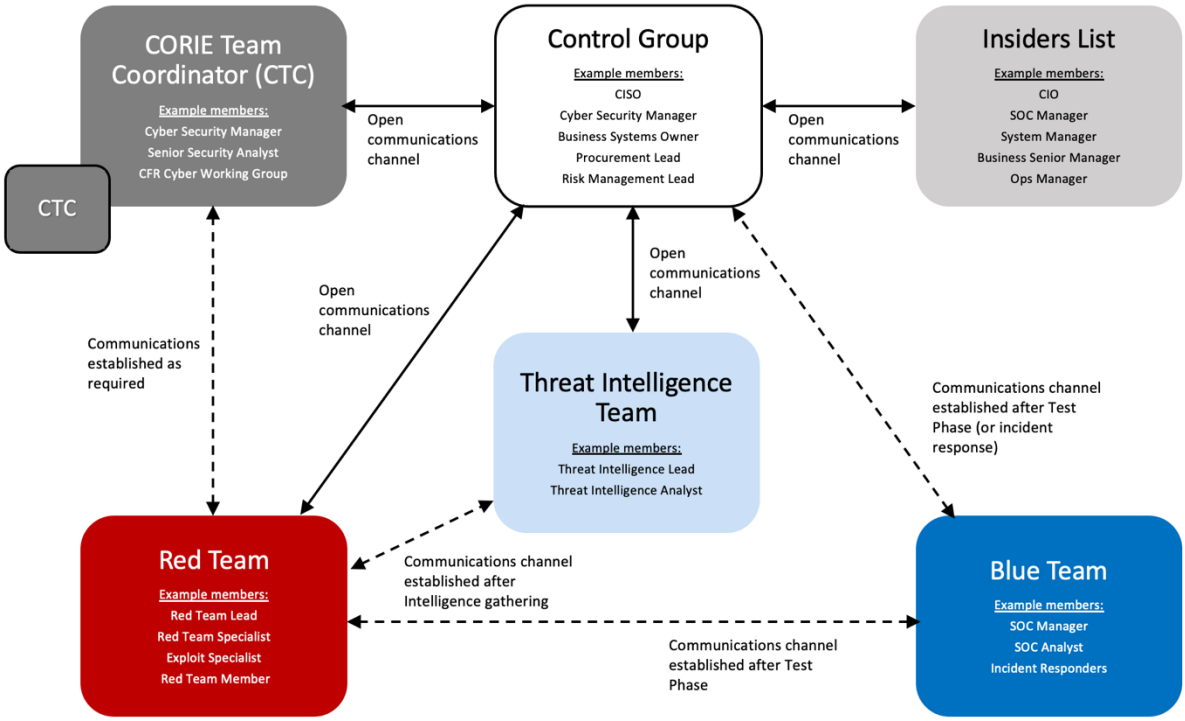


Figure 7 – Control Group communication flow between stakeholders

5.3.2 Threat Intelligence Team

The Threat Intelligence team comprises of team members from a Threat Intelligence Provider. The Threat Intelligence team consists of at least one Threat Intelligence Lead and one Threat Intelligence Analyst. These roles can be fulfilled by the same person.

5.3.3 Red Team

The Red Team consists of at least one Red Team Lead, one Red Team Specialist, one Exploit Development Specialist and optional Red Team Members.

5.3.4 Blue Team

The Blue Team refers to the FI's cyber defence teams. Blue Teams are expected to have no prior knowledge of the exercise, or while activities occur. A senior manager of the Blue Team can be included in the Control Group, providing that effective separation can be guaranteed. However, post exercise debrief meetings between the Provider and Blue Team enable the FI to identify and mitigate any potential gaps within their defences.

5.4 Secrecy and Integrity

The integrity of CORIE is imperative to achieve a holistic view of risks to the cyber resilience and stability of the Australian financial industry.

From initial planning and procurement stages to attack execution, secrecy must be maintained in order to maximise effectiveness of the program.

Ensuring the Blue Team has no knowledge of the adversary attack simulation will make certain that defensive teams do not behave artificially. Secrecy enables the exercise to test how resilient the FI is against real-world adversaries.

The Control Group should be formed early in the Preparation Phase, tasking the team with responsibility of ensuring engagement integrity, particularly through the management of its secrecy.

The exercise should be limited to personnel that have a 'need to know'. Personnel with knowledge of the exercise should be recorded in a trusted insiders list.

Where possible, consider using aliases and code names throughout the exercise. All commonly known terms that provide knowledge of the exercise should be avoided.

5.5 Critical Business Services and Scenarios

Business services are not an individual system but rather a composite of an FI's people, processes and technology supporting a service.

The FI should identify all business services and order them by risk, taking into account if confidentiality, integrity or availability were impacted negatively. The FI should also identify which business services they propose should be in-scope for the exercise, and which should be defined as their Critical Business Services, along with functions that may have a wider systemic impact. Systemically important business services are expected to be those most critical to the stability of the Australian financial markets and financial system.

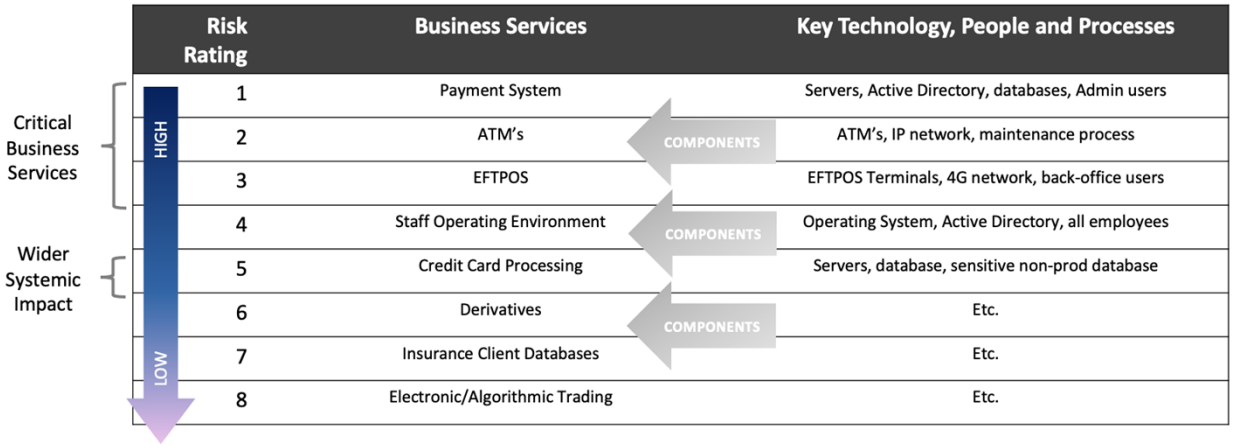


Figure 8 – Example list of Critical Business Services ordered by those most critical to the continued operation of the FI.

The list of Business Services and subset of Critical Business Services should be sent to the CTC for approval.

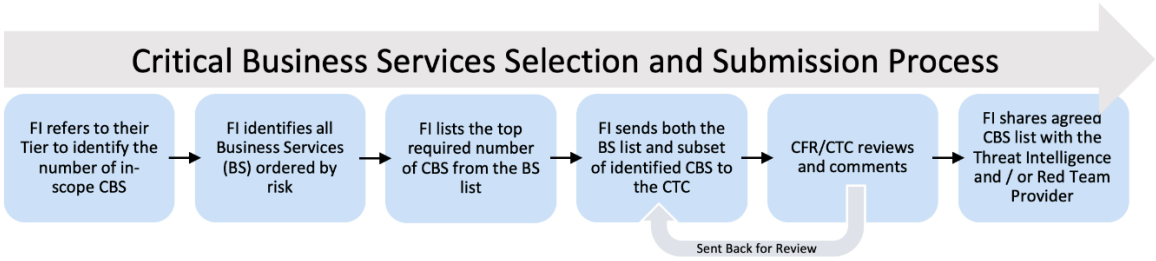


Figure 9 - CBS Selection and Submission Process.

Once the Critical Business Services are agreed they should be provided to the Threat Intelligence provider, as the Critical Business Services shape threat intelligence gathering efforts, which then lead to the creation of Red Team scenarios.

Threat Intelligence focuses on adversaries targeting the approved Critical Business Services. Subsequently, Red Team scenarios must be based on threat scenarios identified by the Threat Intelligence Provider, or those provided by the CTC.

The process of Critical Business Services identification and approval are key to modelling the threats that will provide the greatest value to the FI should the Red Team simulating the modelled scenario have any level of success.

In order to do this, Red Teams use Threat Intelligence reports (where they exist) and or CTC provided scenarios to create the Red Team scenarios. These scenarios are written from the threat actor's point of view, detailing attack paths the Red Team should follow in order to mimic the threat actor when targeting Critical Business Services.

Where possible, details of tactics, techniques, and procedures similar to those simulated adversaries should be included. However, Red Teams should not be limited – new and alternate tactics, techniques, and procedures can be used if required.

Achievement Flags can be placed on people, process and technology that underpin the targeted Critical Business Services.

Achieved Flags will act as indicators to the Control Group that the Red Team is broadly acting within the scope of the engagement, and indicate a level of progress within the exercise.

5.6 Risk Management

The Attack Preparation (Threat Intelligence) stage poses little operational risk to the FI.

However, the Attack Execution (Red Team) stage simulates adversary's methods within the FI's production network, and if not managed with the appropriate care this could have a negative impact on operational availability, confidentiality, and integrity.

It is the responsibility of the FI to ensure that the Provider has an appropriate Risk Management strategy in place prior to the Attack Execution stage.

As a guideline to reduce risk, the FI (typically the Control Group) should:

- Perform a risk assessment of the scenarios and Test Plan to determine any risks that are too great to be performed in a production environment
- Identify any portion of the scenarios and Test Plan that requires Concessions to reduce unacceptable risk
- Sign-off on all scenarios and Test Plan and accept the risks related to in-scope Flags, and the exercise overall
- Ensure an appropriate Communication Plan (as detailed in section 5.8.2.1) is in place, where discussions and approvals can be requested for actions based on the risk plan.

FI's may require Providers to conduct all red teaming activity on-site as a risk mitigation strategy, perhaps under Control Group supervision. Other approaches could include limiting activity to business hours when it is easier to co-ordinate activities and communicate with relevant business and IT stakeholders.

5.7 Preparation Phase

The Preparation Phase signifies the launch of the exercise.

During the Preparation Phase the CTC engages with all parties participating in the CORIE scheme, while FI's commence scoping their external engagements to select the necessary Provider(s).

The Preparation Phase also includes FI's identifying their Critical Business Services, and considering CFR comments on those Services.

5.7.1 Engagement and Scoping

The FI's Control Group should be assembled during the Preparation Phase.

The FI should complete and return the CRA to assist with determining categorisation into an appropriate CRA Tier level which defines a number of parameters for the exercise, these include:

- What type of Threat Intelligence is required
- The number of scenarios to be simulated
- The number of Critical Business Services that will be targeted.

Threat Intelligence and Red Team Providers must meet the standards set out in this Guide.

The following tables explain engagement and scoping requirements based on the Tier level assessed and determined during the CRA.

5.7.1.1 Cyber Risk Assessment Tier 1

Tier 1 – most risk to the stability of the Australian financial markets and financial system.

The following is a CORIE activity:

Adversary Attack Simulation – Red Team Exercise

Requirement	Value
Scenarios	3 (including 1 Generic Scenario supplied by the CTC)
Critical Business Services targeted	2
Threat Intelligence	• Threat Intelligence supplied by Threat Intelligence Provider • Generic Threat Intelligence supplied by the CTC and shared with the FI and Provider • FI Internal Threat Intelligence shared with FI and Provider
Test Phase calendar duration	Expected to last between 5 to 9 months
CTC	1. Receive the Threat Intelligence Reports for enrichment 2. Review the Red Team scenarios 3. Comment on issues in line with this guide 4. Receive the Red Team Execution Report 5. Receive the FI Remediation Plan

The following is a subsequent activity:

- Replay Adversary Attack Simulation – Purple Exercise
- Crisis Simulation Table Top – Gold Team Exercise.

5.7.1.2 Cyber Risk Assessment Tier 2

Tier 2 – may have an impact on the stability of the Australian financial markets and financial system.

The following is a CORIE activity:

Adversary Attack Simulation – Red Team Exercise

Requirement	Value
Scenarios	1
Critical Business Services targeted	1
Threat Intelligence	• Threat Intelligence supplied by Threat Intelligence Provider • FI Internal Threat Intelligence shared with FI and Provider
Test Phase calendar duration	Expected to last between 4 to 6 months
CTC	1. Receive the Threat Intelligence Reports for enrichment 2. Review the Red Team scenario 3. Comment on issues in line with this guide 4. Receive the Red Team Execution Report 5. Receive the FI Remediation Plan

The following is a subsequent activity:

- Replay Adversary Attack Simulation - Purple Exercise
- Crisis Simulation Table Top – Gold Team Exercise.

5.7.1.3 Cyber Risk Assessment Tier 3

Tier 3 – common systemic weakness may have an impact to the stability of the Australian financial markets and financial system.

The following is a CORIE activity:

Adversary Attack Simulation – Red Team Exercise

Requirement	Value
Scenarios	1 Generic Scenario supplied by the CTC
Critical Business Services targeted	1
Threat Intelligence	• Generic Threat Intelligence supplied by the CTC and shared with the FI and Provider • FI Internal Threat Intelligence shared with FI and Provider • Optional - Threat Intelligence supplied by Threat Intelligence Provider
Test Phase calendar duration	Expected to last between 4 to 5 months
CTC	1. Receive the Threat Intelligence Reports for enrichment 2. Review the Red Team scenarios 3. Comment on issues in line with this guide 4. Receive the Red Team Execution Report 5. Receive the FI Remediation Plan

The following is a subsequent activity:

- Replay Adversary Attack Simulation - Purple Exercise
- Crisis Simulation Table Top – Gold Team Exercise.

5.7.1.4 Cyber Risk Assessment Tier 4

Tier 4 – all other FIs regulated by a member of the CFR.

The following are annual activities:

- Replay Adversary Attack Simulation – Purple Exercise
- Crisis Simulation Table Top – Gold Team Exercise.

The Preparation Phase involves FI's identifying their Business Services, and approval of their Critical Business Services. This process is detailed in section 5.5 Critical Business Services and Scenarios.

Critical Business Services reviewed by the CTC must be provided to the Threat Intelligence Provider (if a Threat Intelligence Provider is deemed compulsory by the CRA Tier requirements) and Red Team Provider. Red Team scenarios will be based on threat scenarios identified in Threat Intelligence Reports.

5.7.2 Procurement

The FI's Procurement Team is responsible for acquiring services of a Provider that meets the minimum certification and experience requirements.

As secrecy is essential, the Procurement Team will be required to ensure secrecy is maintained throughout the entire procurement process.

The Control Group should be responsible for ensuring the level of secrecy for the exercise is understood and adhered to by the Procurement Team.

Providers invited to tender should sign a Non-Disclosure Agreement (NDA) prior to any information exchange, and be prohibited to discuss the exercise outside of the procurement process.

Providers, and their testers, are not required to be physically located in Australia to participate in exercises. During Provider selection, the FI's Procurement Team should consider whether their organisational risk appetite or resourcing policies require Threat Intelligence and Red Team members to be physically located in Australia, perhaps due to data sovereignty concerns.

Providers should be supplied with the FI's CRA Tier Level and subsequent exercise requirements, enabling them to understand at a high level the effort required for the exercise.

After Provider selection has been completed, a Project Initiation Meeting (PIM) should take place to introduce the Control Group to the Threat Intelligence Provider and the Red Team Provider.

FIs should have detailed background checks performed on the Provider's team. Provider background checks typically commence after the Provider(s) successfully obtain a contract for the exercise. The background check process should also maintain a high level of secrecy.

For further information refer to the Appendix A: Procurement Guide.

5.8 Test Phase

The Test Phase consists of the Attack Preparation (Threat Intelligence) and the Attack Execution (Red Team) stages.

5.8.1 Attack Preparation – Threat Intelligence

Threat Intelligence involves the collection and analysis of real-world threats targeting the FI and related Critical Business Services.

This stage consists of the acquisition of Threat Intelligence to shape the scenarios simulated in the Test Phase – Attack Execution (Red Team).

There are a number of different types of Threat Intelligence available. Core types of Threat Intelligence for this stage includes:

- Provider Threat Intelligence
- Internal FI Threat Intelligence
- Government Threat Intelligence
- CTC Generic Threat Intelligence.

Threat Intelligence requirements are dependent on an FI's CRA Tier level.

Attack Preparation stage duration is expected to be approximately 1 month, depending on the type of Threat Intelligence and number of scenarios.

5.8.1.1 Provider Threat Intelligence

Due to the impacts that significant breaches can have upon an FI and financial markets, Provider acquired Threat Intelligence is required by the top tier levels as defined by the FI's CRA.

Threat Intelligence Providers provide additional value to the exercise, complementing other threat intelligence types.

Threat Intelligence gathering should start with a process to understand the FI's in-scope business services and in particular with reference to systemic threats to the Australian financial markets and financial system.

Provider acquired Threat Intelligence must cover two areas:

1. Threat Intelligence: relevant threat actors and probable threat scenarios
2. Targeting: potential attack surfaces across the FI's organisation

The Threat Intelligence report should detail collection and analysis to:

- Summarise the FI's threat landscape
- Assess the level that potential threat actors pose to the FI
- Detail potential threat actors' capabilities and intentions.

The Targeting report should detail the collection and analysis to:

- Summarise the potential attack surfaces across the FI
- Assess the nature and degree of publicly available information which would be of potential value to a threat actor in the conduct of reconnaissance or an attack.

The Threat Intelligence Provider should use mechanisms to attempt to gain threat intelligence and targeting information from the Surface, Deep and Dark Web.

Importantly, if a critical vulnerability is discovered during the Threat Intelligence gathering stage, the Provider should escalate the vulnerability to the Control Group immediately rather than waiting to finalise and submit a final report.

To standardise reporting reports should be aligned to the MITRE PRE-ATT&CK[6] and ATT&CK[7] frameworks.

The TI Provider should, where possible, provide specific TTPs to ensure exact tradecraft is simulated. However, the Red Team should not be limited to explore deviations from those specific TTPs when simulating a scenario, as it is unlikely threat groups will also not innovate and evolve their TTPs.

Sufficient time must be allocated for this phase to enable the Provider to produce evidence-based threat intelligence and targeting information commensurate with the number of required scenarios and Critical Business Services.

Evidence should be added to reports where possible, and may include URLs to articles and other resources, pictures and screenshots, and text-based output from discovered intelligence e.g., redacted public breach data.

Based on the threat intelligence gathered, plausible threat scenarios must be developed for use as the basis of subsequent scenarios simulated in the Test Phase – Attack Execution stage.

Output from the Threat Intelligence Provider must include two evidence-based reports:

1. Threat Intelligence report
2. Targeting report

For consistency between Providers, reports should follow a similar structure as detailed in Annex B: Threat Intelligence-led Adversary Attack Simulation Reports.

The number of Critical Business Services in the report must match the CRA Tier level definitions.

6 https://attack.mitre.org/resources/pre-introduction/
7 https://attack.mitre.org/

5.8.1.2 Internal FI Threat Intelligence

FIs often have a threat intelligence function within their organisation collecting and analysing threat intelligence in various ways. Internal FI threat intelligence may include:

- Public and proprietary information feeds
- Intelligence sharing platforms
- Security monitoring and incident response investigations
- Malware analysis
- Penetration testing reports.

Where Provider acquired Threat Intelligence is required, the FI's Threat Intelligence should be shared with the Threat Intelligence Provider to enrich the information.

Due to the common relationships between FI's internal threat intelligence function and their Blue Team, the acquisition of internal threat intelligence should be gathered in a manner where defensive teams are not alerted to the exercise. Secrecy and integrity must be maintained at all times.

Internal threat intelligence should be shared early within the Attack Preparation phase, and finalised Threat Intelligence Provider reports should have already incorporated FI's internal threat intelligence transparently into the conclusions.

Where Provider acquired Threat Intelligence is not required, or available, an FI's internal threat intelligence should be shared with the Red Team to help define realistic threat scenarios against the approved Business Services. In this case, the FI's internal threat intelligence should be combined with CTC Threat Intelligence.

5.8.1.3 Government Threat Intelligence – CTC Report Sharing

Where Provider acquired Threat Intelligence is required, the Threat Intelligence and Targeting reports should be shared with the CTC as soon as complete. Shared reports enable the CTC to work with CFR members and other Government sources to enrich the information gathered with any additional threat intelligence[8].

The CTC will supply the FI with at least one Government Threat Intelligence-based Scenario for use in the Attack Execution (Red Team) stage.

Any threat intelligence provided by the CTC will be shared using the Traffic Light Protocol (TLP) detailed in Annex F: Traffic Light Protocol[9].

5.8.1.4 Threat Intelligence to Red Team Handover

Red Teams should gain access to Threat Intelligence and Targeting reports for analysis after the Attack Preparation – Threat Intelligence is complete.

If the Red Team Provider differs to the Threat Intelligence Provider, a handover meeting should be held that allows the Red Team to query the Threat Intelligence and Targeting reports.

The Red Team should also gain access to any internal FI threat intelligence in addition to any threat intelligence returned from the CTC.

Where Provider acquired threat intelligence is not required, the CTC will supply the FI with Threat Intelligence and or Threat Intelligence-based scenarios for use in the Attack Execution stage by the Red Team.

The Red Team should work with the Control Group to develop scenarios and document them in a Test Plan.

---

8 Government sources may include the Australian Signals Directorate (ASD) and/or Australian Cyber Security Centre (ACSC)

9 TLP classification levels used in the traffic light protocol (TLP) describe the restrictions on access and use of shared intelligence on each classification level

5.8.1.5 Scenarios and Test Plan

Test Plans should detail threat scenarios converted by the Red Team into realistic and effective Red Team scenarios.

A threat intelligence-based scenario supplied by the CTC should be included in the Test Plan.

Test Plans and scenarios should include Flags. Flags can include people, process and information systems that underpin the targeted Critical Business Service. Flags can be useful for the Control Group to indicate the level of progress against overall objectives. All Flags and scenarios should be mapped against Critical Business Services.

A Test Plan should include the schedule of actions with approximate timelines based on the Flags, scenarios and targeted Critical Business Services.

Test Plans should identify actions and Flags that are high risk, and also include an associated risk management strategy as outlined in section 5.6 Risk Management. This may require the Test Plan incorporating possible Concessions, further outlined in section 5.8.2.4 Concessions.

The Red Team should have resources and skills to simulate an adversary's tactics, techniques, and procedures, and be able to complete the defined scenarios detailed in the Test Plan. Any foreseen inability for the Red Team to achieve a Flag or action in a scenario should include Concessions planning.

The Test Plan or the planned Concessions should be shared with the CTC to ensure they meet the intention of the program.

The Test Plan or the planned Concessions should be considered sensitive and valuable to an adversary, as such, should be shared with the FI and CTC as outlined in section 4.4.4 Report Sharing.

5.8.2 Attack Execution – Red Team

The Attack Execution stage involves the execution of the adversary attack simulation as per defined scenarios documented in the Test Plan. The Red Team Provider will execute the simulation as per the agreed Test Plan.

Red Team Provider staffing requirements defined in section 2.4 should be followed. If a Red Team Lead or Red Team Specialist resigns during the exercise, the Control Group must be informed immediately.

Any queries, escalation or disputes that require CTC involvement should use the Issue Register and Resolution process.

The Attack Execution phase duration is expected to be constrained between 3-8 months, depending on the number of scenarios and business services.

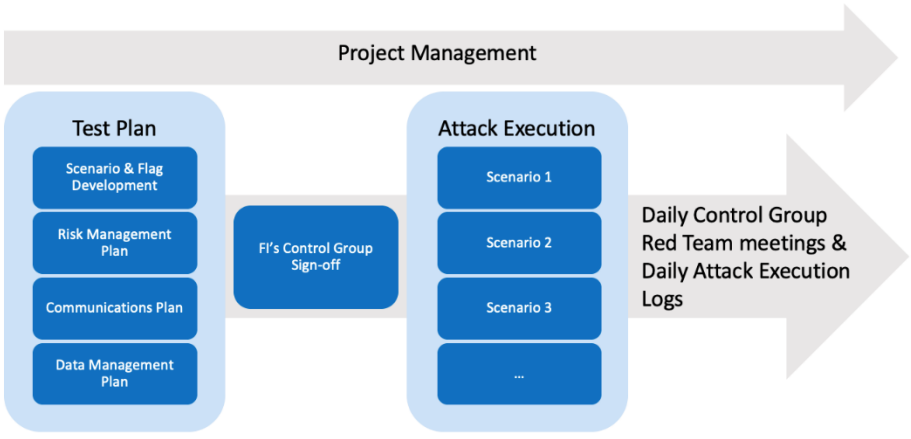


Figure 10 - Components of Attack Execution by the Red Team

5.8.2.1 Communication Plan

A Communication Plan between the Control Group and Red Team should be agreed on prior to the start of the Attack Execution. An Emergency Communication Plan should be part of the Communication Plan.

The plan should include how to communicate in a manner that maintains the secrecy and integrity of the exercise. The importance of the secrecy and integrity of the exercise is outlined in section 5.4 Secrecy and Integrity.

The Emergency Communication Plan must allow the Control Group to contact the Red Team in case of an emergency and vice versa.

The Emergency Communication Plan should include primary and secondary points of contact for both the Control Group and Red Team. It should include different methods of contact for both parties. It is important that 24-hour access to the Control Group and Red Team members is possible during the exercise, as Red Team activity may not be limited to business hours. The Red Team may need to contact the Control Group to inform them of a discovered critical issue or a service disruption. As described previously, if a critical vulnerability is discovered during the Threat Intelligence gathering stage, the Provider should escalate the vulnerability to the Control Group immediately rather than waiting to finalise and submit a final report.

Conversely, an actual attack against the FI may occur out of business hours which requires the Control Group to verify Red Team activity in a timely manner. Additionally, for this purpose, the Control Group should have access to frequent updates of Red Team activity in the form of an Attack Execution Log.

A means to communicate and share sensitive information securely between the Red Team and Control Group should be established e.g., when sharing details of the Attack Execution Log. Sharing of sensitive information should be managed appropriately as outlined in section 4.5 Data Management.

5.8.2.2 Attack Execution Log

The Red Team should maintain details of their activity throughout the exercise, with all actions logged in an Attack Execution Log.

Capturing all actions in an Attack Execution Log, including any deviations from defined attack plans, assists FIs to reverse or repair any changes to their systems that were performed during the attack execution.

The Attack Execution Log will be used to share attack activity details with the Control Group, and for analysis by a Blue Team in the debrief meetings during the Closure Phase. The Red Team should record any actions that require work to clean up within the Attack Execution Log.

The Attack Execution Log should contain detailed actions in a chronological order. Section 9.3.3 Attack Execution Log Report outlines details that are expected to be captured in the Attack Execution Log and submitted as the final Attack Execution Log Report.

All data created or acquired as part of exercise should be managed appropriately as outlined in section 4.5 Data Management.

5.8.2.3 Control Group and Red Team Regular Update Meetings

Control Group and Red Teams are recommended to hold update meetings regularly. During periods of increased activity, daily catch-up meetings are suggested to keep the Control Group informed.

Test Plans, Communication Plans and Risk Management Plans should be followed until the exercise is complete.

5.8.2.4 Concessions

Concessions are a means of transparently assisting the Red Team during the exercise.

Commonly, a Concession will help the Red Team progress to the next Flag in the Test Plan should the Red Team not achieve the objective in a reasonable time.

However, a Concession can be provided to facilitate risk reduction e.g., a Flag or action planned by the Red Team on a production server is deemed too high risk by the FI's Control Group. Instead, the Red Team is provided the

equivalent access to a non-production instance to test the action. On success, the Red Team might be granted the equivalent access back on the production system to continue to the next Flag.

Concessions must be authorised by the Control Group.

Concessions will typically facilitate:

- Providing additional information
- Simulating attaining a Flag / Objective
- Improving efficiency of the exercise
- Preventing premature disclosure of the exercise.

The Control Group is responsible for organising and communicating the details of approved Concessions to the Red Team.

Concessions should be:

- As close to the equivalent simulated achievement as possible
- Without unrealistic challenges or obstructions
- Implemented in a timely manner.

Example Concessions might include:

- Gaining a foothold on the environment, where one could not be obtained in a reasonable timeframe
- Listing staff names and emails, where external reconnaissance was insufficient
- Allowing command and control domains, where egress controls were restrictive
- Providing a position that adversaries may acquire without having to adhere to moral, ethical and legal boundaries.
- Sharing information to improve project timelines e.g., Network diagrams, hostnames, routing information, privilege levels, target application names, where internal reconnaissance is timely and or challenging
- Providing persistence to the environment through remote access or a workstation without a particular security control, where controls could not be bypassed
- Providing privileged access to a specific Flag (system) where one could not be obtained in a reasonable timeframe
- Disclosing PIN or credentials to bypass a laptop's full disk encryption, where controls could not be bypassed
- Sharing information on target business services and systems which underpin them, where internal reconnaissance resulted in insufficient information to progress
- Suppressing escalation of an investigated detection event preventing premature disclosure of the exercise e.g., to an external incident response provider.
- Providing non-production access to complete an action, where the same action in production is deemed too high risk.

Any alteration to a Scenario by virtue of an approved Concession must be documented in detail in the Execution Report.

5.8.2.5 Detection and Response

Red Teams can measure the effectiveness of Blue Teams in detecting their actions.

During the Attack Execution phase the Blue Team may have detected simulated malicious activity, and therefore responded appropriately according to their procedures, such that the Red Team can form a view towards their mitigation capability. Where this is not the case, then the Red Team can seek approval from the Control Group to make increasingly noisy actions until detection, this usually occurs towards the end of the engagement.

This technique will allow the Red Team to evaluate and note the effectiveness of the Blue Team's detection capability, and for the Blue Team to start any detailed investigation.

5.9 Closure Phase

The CORIE Closure Phase comprises the Red Team sharing Attack Execution (log) activity, finalising the Attack Execution report, and conducting debrief meetings with the FI and CTC.

Additionally, the Red Team will replay specific attacks identified as potential weaknesses in the FI's cyber defences.

Closure phase duration typically should be 5 weeks.

The Closure Phase signifies completion of the Attack Execution stage. The end of the Attack Execution stage should be clearly communicated between the Control Group and Red Team.

No further Attack Execution activity should be conducted by the Red Team when the test stage closure has been reached, and agreed upon by both teams.

As the Blue Team were not informed that the exercise was happening, the Control Group should now inform the Blue Team of the exercise details, which includes sharing Threat Intelligence, scenarios and Test Plan and Attack Execution Log Report.

Although the Attack Execution stage has ended, the information is still sensitive and should be shared securely between the Red Team, Control Group and Blue Team. This sensitive information should be managed appropriately.

While the Blue Team are working on a remediation plan, the Red Team will finalise the Attack Execution report in preparation for two debrief meetings.

Debrief meetings are to be conducted by the Red Team, including:

- Blue Team Debrief Meeting
- FI Executive Debrief Meeting.

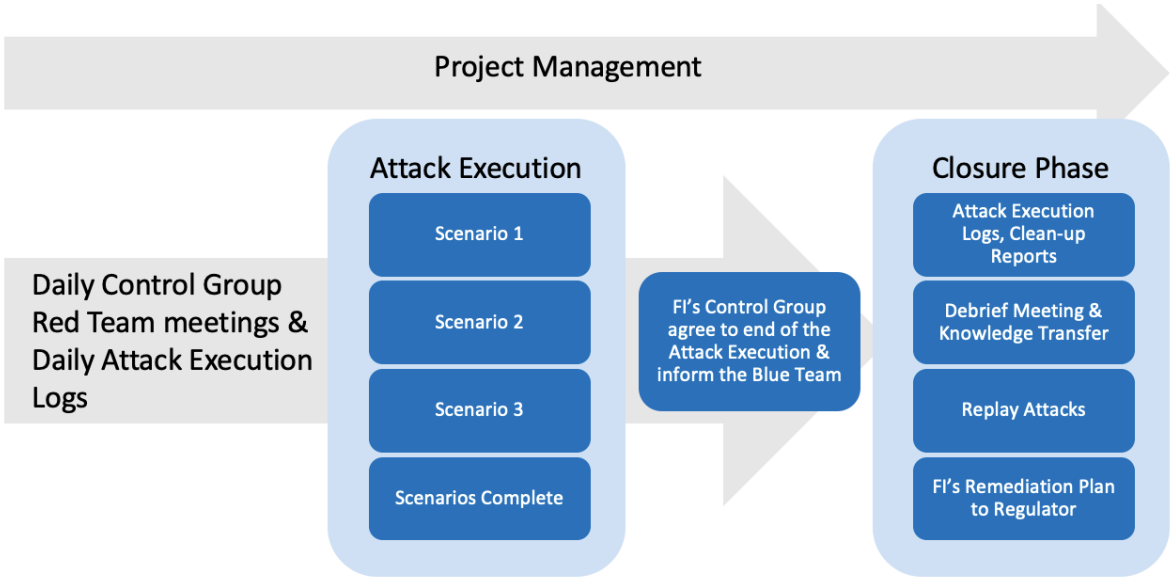


Figure 11 - The Closure Phase signifies completion of the Attack Execution stage

The Closure Phase process should follow the sequence below:

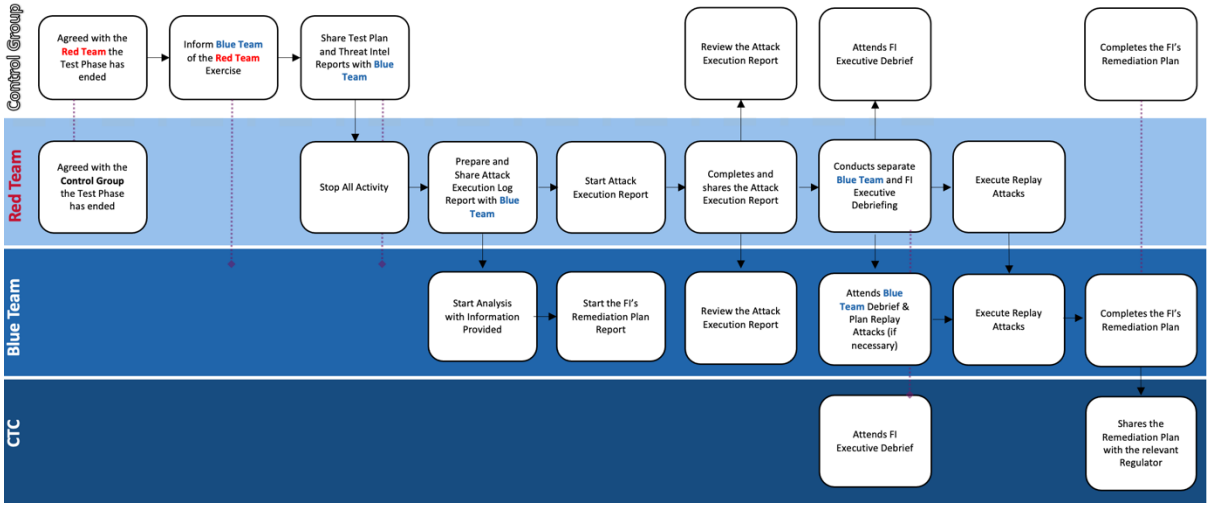


Figure 12 - The Closure Phase will involve the Red Team debriefing the Control Group, Blue Team, CTC and relevant Regulator.

5.9.1 Reporting Remediation and Planning

5.9.1.1 Attack Execution Log Report

An Attack Execution Log forms the basis for the Attack Execution Log Report, which is shared with the Blue Team at the beginning of the Closure Phase – Reporting and Remediation Planning stage. Note that in the Attack Execution Stage, the Red Team were to maintain an Attack Execution Log detailing all activity that occurred.

Attack Execution Log Reports should include chronologically logged actions conducted against the FI from the Attack Execution Log.

The Attack Execution Log Report will help the Blue Team identify attacks that should be considered as in-scope for the Replay Attacks stage.

5.9.1.2 Clean-up Report

While creating the Attack Execution Log Report, the Red Team should record any actions requiring work by the FI to return their environment back to an original pre-test condition. These actions should be captured in a section of the Attack Execution Log Report titled the Clean-up Report.

The Clean-up Report covers anything the Red Team could not clean-up on their own.

The Clean-up Report should include the necessary detail required by the FI to clean up the environment in full i.e., steps required to perform the clean-up activity.

The Attack Execution Log Report and Clean-up Report contain sensitive information. These reports, as well as all data created or acquired as part of exercise, must be managed appropriately as outlined in section 4.5 Data Management.

Details expected to be captured and submitted in the Attack Execution Log Report are covered in section 9.3.3 Attack Execution Log Report.

At the end of the Test Phase, the Attack Execution Log Report and Clean-up Report should be provided to the Control Group.

5.9.1.3 FI's Remediation Plan Report

An FI's Remediation Plan Report should summarise key risks identified within the Red Team report after Replay Attacks have completed – all findings should be included with a risk management based overlay.

The focus of the Blue Team should be to analyse the finalised Red Team Attack Execution Log Report using the scenarios and Test Plan. These documents will help the Blue Team understand the approach and intended flow of events, and the Attack Execution Log Report should enable correlation of events with the FI's detective and preventive controls, security information and event management (SIEM), investigation outcomes and any incident response actions taken.

After the Blue Team have analysed the Red Team's activity they will identify where any gaps may exist. The Blue Team should use those findings to form the outline of the FI's Remediation Plan and include them in upcoming Replay Attacks yet to be conducted.

Remediation Plans should be updated and finalised after delivery of the Attack Execution Report, the Blue Team Debrief Meeting, and conclusion of Replay Attacks.

An FI's remediation plan should be considered very sensitive and valuable to adversaries, as such should be shared securely as per section 4.5 Data Management. Finalised remediation plans should be shared with the CFR and relevant Regulator.

For consistency between FIs, the remediation plan should follow a similar structure as detailed in section 9.4 FI's Remediation Plan Report.

5.9.1.4 Red Team Attack Execution Report

The Attack Execution Report is the final report published by the Red Team during the Reporting Remediation and Planning stage.

While the Blue Team is reviewing the Attack Execution Log Report and creating the FI's Remediation Plan, the Red Team should complete the Attack Execution Report.

Attack Execution Reports should explain, to both the CTC and FI, how the adversary attack simulation concluded together with any deviations from the approved Test Plan.

Consider aligning reports to the MITRE ATT&CK framework to standardise reporting.

Attack Execution Reports should include an executive summary for the CFR, the relevant Regulator, and senior executives of the FI. Reports should include a summary of the scope, scenarios and results, and any Concessions that were required. This section should also include strategic recommendations to improve defences and overall cyber resilience of the FI. Also, if possible, how the FI benchmarked against industry peers.

The report should have sections for senior executives and technical readers, including the FI's Blue Team who require an understanding of how successful attacks were performed and weaknesses mitigated.

Technical portions of the document should include a technical summary of the attack scenarios that were executed, the Test Plan, and Concessions required.

The detailed technical section of the report should be split out by scenario and include results (successes and failures), identified weaknesses ordered by severity, related remediation advice, and findings that demonstrated effective defence capabilities observed in the detection and response assessment section (both positive and negative).

It is feasible for a particular objective to be unsuccessful as part of an action within a scenario e.g., when data or systems cannot be accessed due to lack of presence of suitable attack paths, or security controls blocking access.

The report should highlight tactics, techniques, and procedures that should be considered for future replay attacks.

Additionally, the report should also make recommendations towards which attacks are most valuable to include in the Replay Attacks phase.

Attack Execution Reports should include a timeline of Red Team actions, listing the attack elements that contributed to the success of the attack e.g., weaknesses discovered that enabled the Red Team to progress to the next Flag. This report is used as the source of information for remediation and replay attack planning.

When the Control Group reviews the Attack Execution Report they should provide their exercise and report feedback. At this point, the Red Team should update the Attack Execution Report with the Control Group's

management feedback. Control Group feedback should be included in the FI's Management Feedback section of the report.

The Red Team Attack Execution Report should be considered sensitive and valuable to an adversary, as such should be shared securely as per section 4.5 Data Management.

Sharing of the finalised Attack Execution Report should follow these steps:

1. The Red Team sends a non-draft version of the report to the CTC and Control Group.
2. The Control Group reviews the Attack Execution Report and provides exercise and report feedback to the Red Team. Feedback should include the Control Group's management summary of the exercise for inclusion in the report.
3. The Red Team updates and finalises the Attack Execution Report including any feedback.
4. The Red Team shares a final version of the report with the CTC and Control Group.
5. The Control Group shares the report with the Blue Team. This occurs prior to the Blue Team Debrief Meeting and FI Execution Debrief Meeting.

For consistency between Providers, the Attack Execution Report should follow a similar structure as provided in section 9.3.4 Attack Execution Red Team - Attack Execution Report.

5.9.1.5 Report Matrix

The following table summarises reports created and used during the Closure phase.

Report	Purpose	Who creates the report	Who receives the report
Attack Execution Log Report	Details all the activity that took place throughout the Attack Execution stage	Red Team	Control Group, Blue Team
Clean Up Report	The Clean Up Report should include the necessary detail required by the FI to clean up the environment in full	Red Team	Control Group, Blue Team
Red Team Attack Execution Report	Attack Execution Reports should explain how the adversary attack simulation concluded	Red Team	CTC, Control Group, Blue Team
FI's Remediation Plan Report	Summarise the primary risks identified from the Red Team's Attack Execution report after Replay Attacks have completed – all findings with a risk management based overlay should be included	Blue Team	CTC, Regulator

5.9.1.6 Blue Team Debrief Meeting

The most important benefit of the adversary simulation is a learning opportunity for the FI to identify and close any defensive gaps which may have been identified during the exercise. This is usually achieved by the Red Team walking the Blue Team through the exercise, specifically the Attack Execution Log Report, scenarios and Test Plan, and Attack Execution Report. Debrief meetings are an opportunity for the Blue Team to ask questions of the Red Team, including outputs into their own draft FI's Remediation Plan.

Combined Red Team and Blue Team analysis enables the FI's defensive teams to identify gaps and improve their defences, those findings should be updated in the FI's Remediation Plan.

A Blue Team Debrief meeting must take place with expectations that relevant members of the Blue Team attend, as well as at least one member representing the Control Group.

To help the Red Team prepare for the debrief meeting, the Blue Team can share the FI's draft Remediation Plan prior to the meeting.

The Blue Team should have reviewed the Attack Execution Report prior to the meeting.

This meeting is technical in nature and focuses on:

- A walk-through of the Attack Execution Log Report and Attack Execution Report
- The Blue Team walk-through of their analysis of the above.

Additionally, the meeting is used to identify scope and plan for upcoming Replay Attacks to be conducted by the Red Team.

5.9.1.7 FI Executive Debrief Meeting

FI executive debrief meetings should consist of a Red Team presentation to the CTC, FI's executive team, and Control Group.

The Red Team should send an invitation to the CTC mailbox (detailed Annex A: CTC Contact Details).

This meeting should also provide an opportunity for the FI and Provider to offer feedback to the CTC towards improving and evolving the CORIE guide and scheme.

5.9.2 Replay Attacks

Replaying specific actions will enable the Blue Team to implement, configure or improve detective and preventative controls.

During the Blue Team Debrief Meeting, the Blue Team should have scoped and scheduled any Red Team actions they wish to replay.

Replay attacks involve the Red Team working closely with the Blue Team to perform specific attack actions repeatedly until security controls are configured to detect or prevent unintended actions. Outcomes can also include updating response capability, such as incident response playbooks.

Replaying Red Team actions should be limited to critical and high-risk issues, or specific actions that were chained and led to those findings. Replay duration is expected to be constrained to within a period of two days to a week, with no requirements for the Red Team to update the Attack Execution Report.

At this point, the Blue Team will update the FI's Remediation Plan including improvements gained from completed replay attacks. An updated Remediation Plan should now be shared with the CFR and relevant Regulator.

6. Replay Adversary Attack Simulation - Purple Exercise

A Purple Exercise should be completed by Tier 1, 2 and 3 FIs annually.

6.1 Summary

Replay attack simulations are intended to measure and improve the prevention, detection and response capability of the FI's defensive teams. These simulations involve a Red Team working with the FI's defensive (Blue) team to repetitiously execute adversary's tactics, techniques, and procedures against the FI's defences.

Replaying attacks helps the Blue Team identify gaps needing remediation and should also reduce the mean time to detect and respond to real adversaries.

A threat intelligence identified adversary's modus operandi simulated in this way provides confidence to the FI, CTC and Regulator that the Blue Team can contain, eradicate and recover from a real event in an acceptable manner.

Internal resources can be used to run a Purple exercise – an independent Red Team Provider is not required. FI's may opt to engage a Red Team Provider if they would like to gain a fresh perspective or do not have available in-house resources.

Note: In the following sections, a Provider can be substituted with internal resources.

Providers must have appropriate resources and skills to simulate the adversary's tactics, techniques, and procedures, and work with the Blue Team to help them understand and remediate any gaps in prevention, detection and response capability.

Duration is expected to last between 10 and 20 days, with a requirement for the Red Team to produce a Replay Attack Report.

The exercise is delivered in five (5) stages:

- Stage 1: Procurement and Project Initiation
- Stage 2: Threat Intelligence
- Stage 3: Replay Attack Plan Development
- Stage 4: Replay Attack Execution
- Stage 5: Replay Attack Report

6.2 Replay Adversary Attack Simulation - Purple Exercise

6.2.1 Procurement and Project Initiation

The FI's Procurement Team is responsible for procuring the services of a Red Team Provider.

The Procurement team should follow the Appendix A: Procurement Guide.

Exercise initiation should commence with a PIM attended by the Red Team Specialist (or equivalent) and the Blue Team.

The PIM's intention is to:

- Confirm objectives
- Confirm the scope of the exercise
- Identify key Threat Intelligence
- Confirm all administrative and logistical details for the exercise
- Agree milestones and timelines.

A Red Team Specialist (or equivalent) should produce a Project Initiation Document (PID). Output from the PIM will be documented and agreed by both parties.

6.2.2 Threat Intelligence

Threat Intelligence requirements for this exercise involve identifying real-world threat actors targeting FIs and understanding their modus operandi.

The intended scope of this exercise involves the Red Team acquiring threat intelligence from the FI and combining that with the CTC supplied threat intelligence scenarios.

Internal FI threat intelligence may include:

- Public and proprietary information feeds
- Intelligence sharing platforms
- Security monitoring and incident response investigations
- Malware analysis
- Penetration testing reports

CTC supplied Threat Intelligence can be requested via email from the CTC mailbox listed in Annex A: CTC Contact Details.

Red Teams should use supplied threat intelligence to create scenarios and determine the tactics, techniques, and procedures that require reproducing, which will formulate the Replay Attack Plan.

6.2.3 Replay Attack Plan Development

After the Red Team have researched and identified in-scope tactics, techniques, and procedures mapping against the Threat Intelligence-led scenarios, these should be detailed in the Replay Attack Plan.

The Replay Attack Plan should plot against a commonly available and widely recognised attack framework, such as the MITRE ATT&CK™[10] framework, or one of the more common Kill Chains[11].

Utilising a common and recognised framework provides a systematic approach that is repeatable with measurable structure, also forming a reusable language across different Providers, the FI's business, Blue Team, and the community.

The Red Team should work with the Blue Team to identify high risk actions which may require creating a risk management plan prior to executing attacks. The risk management plan should be documented in the Replay Attack Plan.

The Blue Team should approve the Replay Attack Plan prior to execution.

6.2.4 Replay Attack Execution

The Red Team should execute the Replay Attack Plan, working closely with the Blue Team to support them understanding and remediating gaps in their prevention, detection and response security controls.

During the course of execution, any deviation to the Replay Attack Plan should be clearly detailed in the Replay Attack Report. These deviations could include moving from testing in a production environment to non-production due to a potential negative impact on business services, or the failure to complete an attack in the plan.

---

10 MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Further information is available at https://attack.mitre.org

11 For example, the Cyber Kill Chain® framework developed by Lockheed Martin. Further information is available at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

6.2.5 Replay Attack Report

Replay Attack Reports should follow a format similar to example in Annex C: Replay Adversary Attack Simulation Reports.

The framework used in the Replay Attack Plan should be documented in the Replay Attack Report. The framework should be used to show the current prevention, detection, and response capability, as well as improvements in time and coverage.

Risk mitigation or deviations from Replay Attack Plan should be clearly detailed in the Replay Attack Report.

Replay Attack Reports should be considered sensitive, and valuable to a threat actor, as such should be shared with the FI as per section 4.5 Data Management, and with the CTC as outlined in section 4.4.4 Report Sharing.

7. Crisis Simulation Table Top - Gold Team Exercise

A Gold Team Exercise should be completed by all Tier 1, 2 and 3 FIs at least annually.

7.1 Summary

Crisis simulation Table Top based exercises assess and improve the FI's internal and external communications, crisis management procedures and senior management decision-making ability in preparation for a real cyber incident.

Internal resources can be used to run a Gold Team exercise – an independent Red Team Provider is not required. FI's may opt to engage a Red Team Provider if they would like to gain a fresh perspective or do not have available in-house resources.

Note: In the following sections, Provider can be substituted with internal resources.

Crisis simulation Table Top exercises involve the Provider (or internal resources) assessing the FI's senior executives, generally the team that forms the FI's crisis management team. The Provider simulates adversary attack scenarios in a structured 'Table Top' based exercise, safe in the knowledge that the attack can be discussed and managed appropriately.

The crisis management team are expected to respond according to their cyber incident response plan, playbooks and processes, while the Provider assesses their actions, and identifies recommendations for improvement.

Exercises include testing communication plans between Board, management and shareholders, ensuring that correct messages are passed in a timely manner between the business stakeholders. Additionally, the exercise should assess external communications provided by the internal communication team to social media, authorities and media.

Assessing the crisis management team in this manner provides the Regulator and FI confidence that the crisis management team can handle a 'real-world' cyber incident in an appropriate manner. Sound management of cyber-incidents provides confidence and assurance that the business can continue operating, risks are appropriately managed, and stakeholders are fully informed.

Key objectives of the exercise are:

- Analysis of the existing internal and external communication processes and protocols in dealing with a cyber-security incident
- Identifying areas for improvement to the communication processes and protocols to ensure best practice preparedness for communicating effectively during and post an incident
- Test the effectiveness of the Executive team's roles and responsibilities in testing the agreed crisis communications processes and protocols
- Familiarise the Executive team with best practice in implementing these processes in a simulated cyber breach scenario
- Test participants under a degree of pressure and enable the identification of potential weaknesses within the crisis management team where greater training and familiarity may be required

Gold Team exercise duration is expected to last for approximately 5 days, with a requirement for the Gold Team to produce an assessment of the Incident Response Exercise Report.

The exercise should include six (6) stages:

- Stage 1: Procurement and Project Initiation
- Stage 2: Threat Intelligence
- Stage 3: Scenario and Inject Development
- Stage 4: Pre-exercise Facilitation

- Stage 5: Crisis Simulation Table Top Exercise
- Stage 6: Incident Response Exercise Report

7.2 Crisis Simulation Table Top Exercise

7.2.1 Procurement and Project Initiation

The FIs' Procurement Team is responsible for procuring the services of a Gold Team Exercise Provider.

Provider selection processes should be fair and transparent, and any questions asked by a Provider should be shared to all parties. The Procurement team should follow the Appendix A: Procurement Guide.

Project initiation should commence with a PIM facilitated by the Gold Team Lead and representative of the crisis management team.

The PIM should:

- Confirm the objectives
- Confirm the scope of the exercise (e.g., IT teams only or engagement with business operations and external authorities)
- Confirm all administrative and logistical details
- Agree phase milestones and timelines.

The Gold Team Lead should produce a PID. Output from the PIM will be documented and agreed by both parties.

7.2.2 Threat Intelligence

Threat Intelligence requirements for this exercise involve identifying real-world threat actors targeting the FI and understanding their modus operandi.

Intended scope of this exercise includes the Gold Team Lead acquiring threat intelligence from the FI, and combining this intelligence with the most recent government Threat Intelligence defined scenarios supplied by the CTC.

Internal FI threat intelligence may include:

- Public and proprietary information feeds
- Intelligence sharing platforms
- Security monitoring and incident response investigations
- Malware analysis
- Penetration testing reports

CTC supplied Threat Intelligence can be requested via email from the CTC mailbox listed in Annex A: CTC Contact Details.

7.2.3 Scenario and Inject Development

A Gold Team Lead should research any identified threat actors and scenarios to determine the type of scenarios used to test the incident response plan. Scenarios are to be tailored to FI business operations ensuring that specific incident response processes and procedures are effectively tested, along with the respective Business Services roles and responsibilities involved in the process. This will enable the Provider to develop a Main Events List (MEL) and accompanying injects for the exercises:

- The MEL is a detailed explanation of the activities and the controls that form the exercise e.g., a description of the attack and compromise vector and the attack objective; a description of intended business impact and response activity; and, an exercise timeline

- Accompanying injects are information artefacts that will be fed into the exercise through a pre-determined channel, along the exercise timeline and to certain participants in order to progress the incident
- The events and responsible roles will be developed further into an exercise script, with will enable the facilitation of the smooth outcome of the exercise.

7.2.4 Gold Team Pre-Exercise Facilitation

A Gold Team Lead should complete a preparatory workshop to ensure that all FI's stakeholders involved in the exercise are aware of the objectives, outcomes, methodology, control measures and have a copy of their incident response plan and any specific playbooks necessary to achieve the exercise objective.

7.2.5 Crisis Simulation Table Top Exercise

The Gold Team Lead will facilitate the structured Table Top exercise whereby the FI's stakeholders respond according to their Cyber Incident Response Plan, playbooks and processes.

The Gold Team Lead should be supported by another technical and risk-based team member(s) to help facilitate the progress of the exercise, identify MEL injects for the exercises, and observe and record the recommendations for improvement.

The onsite exercise should run for no more than a working day, and follow these stages:

- Role introductions
- Exercise objectives and approach
- Exercise Rules of Engagement
- Incident Response Table Top Exercise
- Incident Response feedback and discussion points

7.2.6 Gold Team Incident Response Exercise Report

The FI will receive a business focused Incident Response Exercise Report providing detailed observations and recommendations based on the findings from the exercise.

Incident Response Exercise Reports should follow a similar format to that detailed in Annex D: Crisis Simulation Table Top Reports.

Incident Response Exercise Report should be considered sensitive and valuable to an adversary, as such, should be shared with the FI as per section 4.5 Data Management and with the CTC as outlined in section 4.4.4 Report Sharing.

8. Annex A: CTC Contact Details

The CTC can be contacted by emailing: corie@rba.gov.au

9. Annex B: Threat Intelligence-led Adversary Attack Simulation Reports

For consistency between Providers, the following reports should follow a similar structure as detailed here.

9.1 Threat Intelligence – Threat Intelligence Report

The Threat Intelligence Report contains information on relevant threat actors and probable threat scenarios. Threat Intelligence report should detail the collection and analysis to:

- Summarise the FI's threat landscape
- Assess the level that potential threat actors pose to the FI
- Detail potential threat actors' capabilities and intentions that are targeting the FI

The report should follow a structure similar to:

- Executive Summary
- Scope
  - Objectives
  - Critical Business Services
  - Research Methods
  - Ethical Statement
- Overview of FI's Critical Business Services
- Overview of FI's Threat Landscape
  - Threat Matrix **
- Threat Profiles
  - *threat profile name [1]*
    - Threat Summary
    - Goal Orientation
    - Target
    - Capability
    - Modus Operandi
    - Activity
  - *threat profile name [2]*
    - *etc.*

**The Threat Matrix and table should provide a visual representation of the overall threat landscape. The matrix should plot identified threat actor with their classification/objective according to their threat (Capability x Intent).

Intent \ Capability	Very Low	Low	Medium	High	Very High
Negligible	Low	Low	Low	Medium	Medium
Low	Low	Low	Medium	Medium	High
Medium	Low	Medium	Medium	High	High
High	Medium	Medium	High	High	Very High
Very High	Medium	High	High	Very High	Very High

Figure 13 - Example Threat Matrix

Threat Actor	Threat Description	Capability	Intent	Threat Rating
APT38	APT38 is a financially-motivated threat group that is backed by the North Korean regime. The group mainly targets banks and financial institutions and has targeted more than 16 organizations in at least 13 countries since at least 2014.	Very High	High	Very High
Cobalt Group	Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia.	Very High	High	Very High

Figure 14 - Example Threat Matrix Table

9.2 Threat Intelligence - Targeting Report

The Threat Intelligence Targeting Report contains information on potential attack surfaces across the FI's organisation. The Targeting Report should detail the collection and analysis to:

- Summarise the potential attack surfaces across the FI
- Assess the nature and degree of publicly available information which would be of potential value to a threat actor in the conduct of reconnaissance or an attack.

The targeting report should follow structure similar to:

- Executive Summary
- Scope
  - Objectives
  - Critical Business Services
  - Targeting Methods
  - Ethical Statement
- People
- Processes
- Infrastructure
- Technical Infrastructure

9.3 Attack Execution Red Team – Attack Execution Log and Report

The Attack Execution Log Report should include the chronologically logged actions against the FI from the Attack Execution Log, the Clean-up Report and additional summaries.

9.3.1 Attack Execution Log

The Attack Execution Log should log detailed actions conducted by the Red Team against the FI in a chronological order. A detailed Execution Log should include:

- Details of each action in chronological order:
  - Date and time
  - Red Team member
  - Actions taken and type of attack
  - Success or fail, and success criteria (e.g., Flag achieved)
  - Details of targets including staff name, IP address, machine names, and application names
  - Details of any processes, commands, compiled binaries executed etc.
  - Description of any exfiltrated data
  - Detailed notes of any artefacts left behind (also noted in the Clean-up Report).

9.3.2 Clean-up Report

The Clean Up Report should detail any actions that require work from the FI to clean up at the end of the Attack Execution (Red Team) phase.

The Clean Up Report should include as much detail as possible including the steps required to perform the clean-up activity.

9.3.3 Attack Execution Log Report

The finalised Attack Execution Log Report should include:

- A summary of the timeline
  - Scenarios simulated with outcomes – success/failures
  - Concessions
- A timeline of key events with details of hosts accessed and C2 processes ran
- Attack Execution Log
- The Clean Up Report

9.3.4 Attack Execution Red Team - Attack Execution Report

The report should follow a structure similar to:

- Executive Summary
  - Scope
  - Scenarios and Results
  - Strategic Recommendations
  - Industry Benchmark (if possible)
  - FI's Management Feedback
  - Risk Matrix **

- Technical Summary
  - Attack Scenarios Executed
  - Test Plan
  - Concessions
- Scenario Results
  - Overall Scenario Summary
    - Actions on Critical Business Services Results
    - Detection and Response Assessment
    - Systemic Weaknesses and Recommendations
  - *Scenario [1]*
    - Summary
    - Attack Details (by severity incl. positive controls or Red Team attack failures)
    - Recommendations
  - *Scenario [2]*
    - etc
- Appendices
  - Supplemental Data
  - Replay Attack Recommendations

**The Risk Matrix used for all issues should provide an easy way to identify the risk for each weakness or vulnerability discovered.

Each issue should be assigned a risk rating by the Provider according to a Risk Matrix containing qualitative ratings for the two dimensions of risk – likelihood and consequence.

The following table shows the ratings used when determining the level of risk. The indicator chosen should reflect the likelihood and consequence ratings. There are five risk ratings: very low, low, medium, high and very high.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	Low	Medium	High	Very High	Very High
	Likely	Low	Medium	High	Very High	Very High
	Possible	Very Low	Low	Medium	High	High
	Unlikely	Very Low	Very Low	Low	Medium	Medium
	Rare	Very Low	Very Low	Low	Low	Medium

Figure 15 - Example Risk Matrix

The following table can be used when determining a rating for the consequence of a particular event:

Consequence Rating	Description
Catastrophic	Severe business disruption; very large financial loss; very serious public reputation damage
Major	Partial disruption to the business area; injury to personnel; large financial loss; reputation damage with specific customers
Moderate	Disruption but still able to continue business; moderate financial loss; some public embarrassment
Minor	Small financial loss; some disruption to daily work flow
Insignificant	Inconvenient or minimal effect; no injuries, no financial loss

The risk of these issues should map to the following recommendation mapping:

Likelihood Rating	Description
Almost Certain	Expect to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might reasonably be expected to occur at some time
Unlikely	Could occur at some time, given a particular set of circumstances
Rare	May only occur in exceptional circumstances

9.4 FI's Remediation Plan Report

The FI's Remediation Plan Report should summarise the primary risks identified in Red Team report after Replay Attacks.

The FI's Remediation Plan Report should include all findings with a risk management based overlay.

The FI's Remediation Plan Report should follow a similar structure as:

- A management remediation plan to address any residual risk to the FI
- Summary
    - Primary Risks Identified
    - Closed Risks (remediated, accepted, or mitigated)
    - Defensive Improvement Plan
    - Systemic Weakness Improvement Plan
- Detailed Analysis
    - Defensive Improvement Plan
        - Prevention
        - Detection
        - Response
    - Risk Remediation Plan
        - People
        - Processes
        - Technology

10. Annex C: Replay Adversary Attack Simulation Reports

10.1 Replay Attack Report

The Replay Attack Report must include an Executive summary for senior executives. This should include a summary of the scope, scenarios exercised, result against the selected framework, and any recommendations.

The technical portion of the report should include a detailed scope from the Replay Attack Plan, any caveats that prevented testing as per the plan, detailed scenario-based tactics, techniques, and procedures exercised, and results against the selected framework. The result should feature the current prevention, detection, and response capability, as well as any identified gaps and recommendation for improvements in time and coverage.

Reports should follow a structure similar to:

- Executive Summary
  - Scope
    - Scenarios Exercised
    - Framework Result[12]
    - Recommendations
- Technical Summary
  - Detailed Scope – Replay Attack Plan
  - TTPs Assessed
  - Framework Results and Recommendations
- Appendices
- Supplemental Data

12 Framework Result should include a visual representation of the assessed detection and response capability against technique, tactics and procedures exercised. For example, that may include a detection and response capability heat diagram overlay to the Mitre ATT&CK technique and tactics.

11. Annex D: Crisis Simulation Table Top Reports

For consistency between Providers, the following reports should follow a similar structure as detailed here.

11.1 Incident Response Exercise Report

The Crisis Simulation Table Top Report contains information on the outcome of the Table Top Exercise, with recommendations for improvement.

The report should detail the collection and analysis to:

- Summarise high risk findings and recommendations
- Actions for management
- Detailed analysis of the cyber incident plan and its processes

The report should follow a similar structure as:

- Executive Summary
- Scope
  - Objectives
  - Roles involved in the exercise
  - Scenarios tested
- Overview of the FI Business Services processes
- Details of the findings and recommendations, focussing on people and processes and how they operated
- Sections on incident:
  - Identification
  - Containment
  - Eradication
  - Recovery

12. Annex E: References

12.1 Legal Disclaimer and Copyright Notice

Relevant frameworks and industry peers were consulted in the creation of this guide. These include:

- CBEST Intelligence-Led Testing – CBEST Implementation Guide version 2.0[13]
- Singapore ABS Red Team Adversarial Attack Simulation Exercises Guidelines v1[14]
- TIBER Threat Intelligence Based Ethical Red teaming - TIBER-NL GUIDE 2.0[15]

This document, the *CORIE Framework v2.0*, contains material adapted from material to which the Bank of England ("BoE") owns the copyright, being the BoE's CBEST Intelligence-Led Testing document (the "BoE Licensed Material") as licensed by BoE under the Creative Commons Attribution 4.0 International License, - a copy of which can be found on http://creativecommons.org/licenses/by/4.0. The BoE Licensed Material contains a disclaimer of warranties.

This CORIE guide, contains material adapted from material to which the De Nederlandsche Bank ("DNB") owns the copyright, being the DNB's TIBER Threat Intelligence Based Ethical Red teaming - TIBER-NL GUIDE 2.0 document (the "DNB Licensed Material") as licensed by DNB under the Creative Commons Attribution 4.0 International License, a copy of which can be found on http://creativecommons.org/licenses/by/4.0. The DNB Licensed Material contains a disclaimer of warranties.

13 https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide

14 https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

15 https://www.dnb.nl/en/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm47-365455.pdf?2019092501

The following form of attribution of RBA Material is required:

Source: Reserve Bank of Australia [year] OR **Source**: RBA [year]

This CORIE guide is intended as a general reference for users. It is made available on the understanding that the RBA, as a result of providing this information, is not engaged in providing professional or financial advice.

The RBA accepts no responsibility for the accuracy or completeness of this CORIE guide and recommends that users exercise their own care and judgment with respect to its use.

Users of this CORIE guide assume the entire risk related to their use of such materials, including the use of any materials as the basis for a transaction or any other commercial activity. The RBA does not accept any liability arising from reliance on or use of this CORIE guide.

The RBA does not endorse or promote any transaction or other use (be that commercial or non-commercial) that references or relies on this CORIE guide. The RBA expressly disavows any use of this CORIE guide that in any way violates any applicable law or regulation in force in Australia or a foreign country (or any part of Australia or a foreign country).

The RBA is not, under any circumstances, liable for damages of any kind arising out of or in connection with use of or inability to use this CORIE guide, including damages arising from negligence on the part of the RBA, its employees or agents. By using this CORIE guide, the user agrees to waive all claims against the RBA and its officers, agents, and employees from any and all liability for claims, damages, costs and expenses of any kind arising from or in any way connected to use of this CORIE guide, including claims arising from negligence on the part of the RBA, its employees or agents.

Any use of materials provided under the CC BY 4.0 Licence are additionally subject to the disclaimers and warranties as set out in that licence. The terms and conditions can be accessed at: https://creativecommons.org/licenses/by/4.0/legalcode.

13. Annex F: Traffic Light Protocol

The following table lists the classification levels used in the traffic light protocol and describes the restrictions on access and use of intelligence for each classification level.

Colour	When should it be used?	How may it be shared?
RED	Information should be marked as RED when it cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused	DO NOT SHARE WITH OTHERS Recipients must not share RED marked information with any parties outside of the specific information exchange, meeting or conversation in which it is originally disclosed.
AMBER	Information should be marked as AMBER when information requires support to be effectively acted upon, but carries risk to privacy, reputation, or operations if shared outside of the organisations involved.	DO NOT SHARE OUTSIDE OF THE ORGANISATION Recipients may only share AMBER marked information within their own organisation who need to know, and only as widely as necessary to act on that information.
GREEN	Information should be marked as GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector.	SHARE WITH PEERS/PARTNERS PRIVATELY Recipients may share GREEN marked information with peers and partner organisations within their sector or community, but not via publicly accessible channels.
WHITE	Information should be marked as WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	SHARE WITHOUT RESTRICTION Recipients may share WHITE marked information without restriction, subject to copyright controls.

14. Annex G: Appendix Document Overview

14.1 Appendix A: Procurement Guide

The CORIE Procurement Guide provides information to ensure that the FI's procurement team has the necessary knowledge to run the procurement process as per the requirements of CORIE.

The Procurement Guide provides tools to help assess and select necessary Providers, as well as how to interact with the CTC and relevant Regulators, efficiently and in-line with some of the unique requirements of exercises e.g., dealing with secrecy throughout the engagement.

Refer to the document titled: CORIE Procurement Guide, available to participating FIs on request from the CTC (See Annex A: CTC Contact Details).

14.2 Appendix B: Provider Guide

The Provider Guide provides information on the standards required to execute exercises detailed in this framework.

The Provider Guide provides information for Providers to ensure they have the necessary experience and certifications to meet the standard, as well as recommended training courses to help achieve the skill required to deliver CORIE exercises.

As industry certifications and recommended training evolves, so too will the separate Provider Guide.

The Provider Guide is also useful for FIs to ensure their Providers meet the necessary experience and certifications.

Refer to the document titled: CORIE Provider Guide, available on the CFR website or on request from the CTC (See Annex A: CTC Contact Details).

14.3 Appendix C: Control Group Guide

The Control Group Guide provides recommendations for FIs on how-to work through the CORIE exercises.

Refer to the document titled: CORIE Control Group Guide, available to participating FIs on request from the CTC (See Annex A: CTC Contact Details).

15. Acknowledgements

The following persons/parties are acknowledged for their contribution in the development of the CORIE Framework:

Tim Dillon
Regional Director GPS - APAC
NCC Group

Heath Rolls
Chief Information Security Officer
Reserve Bank of Australia

Subu Ananthram
Manager, Cyber Security Delivery
Reserve Bank of Australia

Adam Lee
Senior Cyber Security Portfolio Specialist
Reserve Bank of Australia

Daniel Kruzic
Manager, Payments & Industry Cyber Security (-2021)
Reserve Bank of Australia

CFR Cyber Security Working Group
Identities withheld for privacy

CORIE Pilot Program Participants
Identities withheld for privacy