Advisory

Title	OSFI's Intelligence-led Cyber Resilience Testing (I-CRT) Framework
Category	Sound Business and Financial Practices
Date	April 1, 2023
Sector	Banks Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies

Table of Contents

List of figures

List of tables

1. Foreword

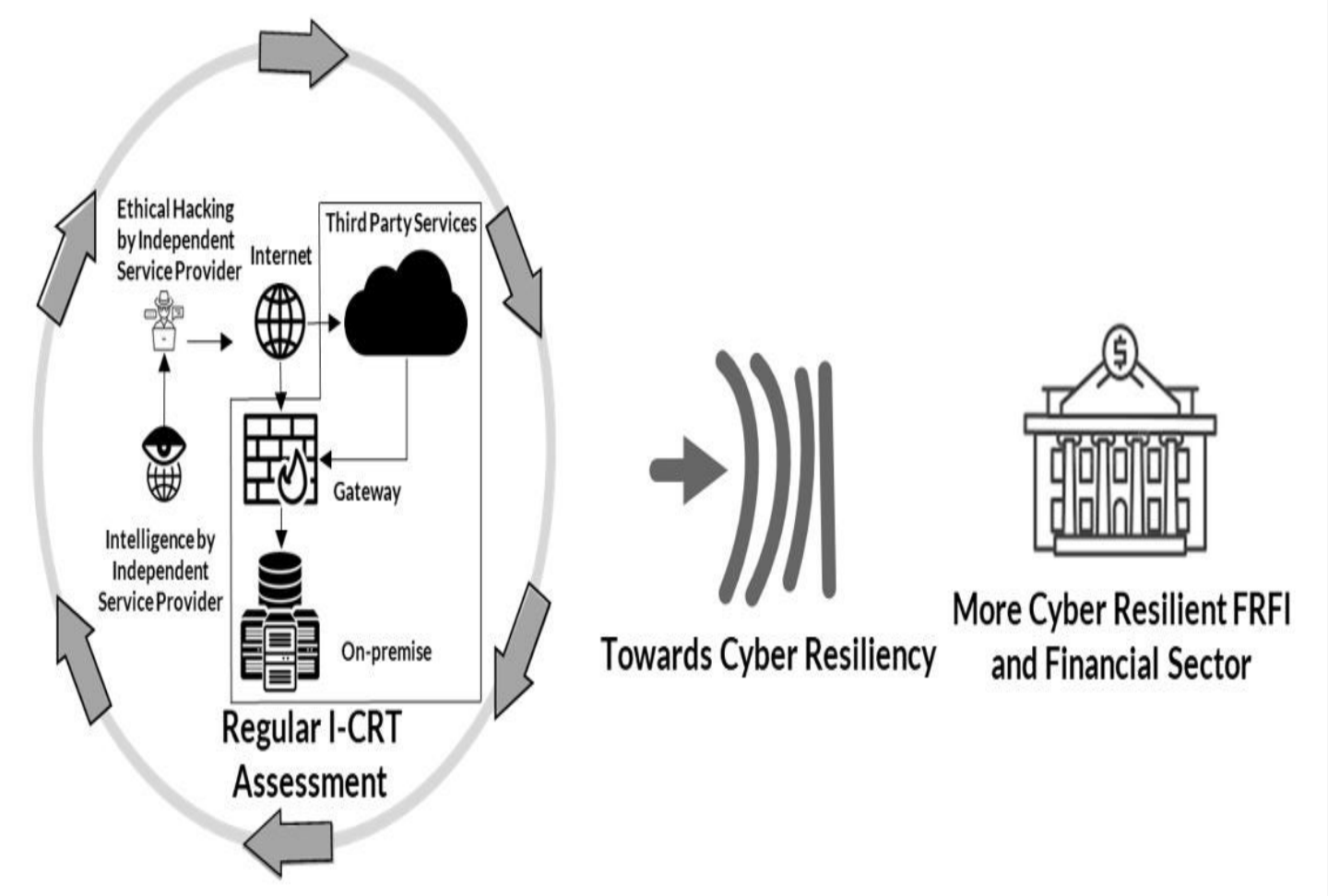
Cyber risk continues to be a top risk faced by many industries, including the financial sector. Cyber attacks can disrupt a Federally Regulated Financial Institution's (FRFI) Critical Business Function (CBF)—even to the point of threatening its viability—or impacting consumers and other market participants in the financial sector. Effectively managing cyber risk is an essential element of a FRFI's cyber resilience. As a supervisory tool, this framework is a "how to" guide to follow when conducting OSFI's Intelligence-Led Cyber Resilience Testing (I-CRT) assessments. This document is not a policy instrument used to set regulatory expectations.

Cyber attacks are increasing in sophistication and severity, amplifying the need to have measures in place that promote resilience to cyber events and technology disruptions. One effective way to build this resilience comes from adopting the mindset of a threat actor when conducting red team testing with quality intelligence to mimic a real-world setting. The I-CRT framework is a controlled, bespoke, intelligence-led test of a FRFI's underlying technology assets and services supporting CBFs. An I-CRT assessment of a FRFI is a regulatory-led (i.e., OSFI) activity where OSFI provides guidance and oversight throughout the assessment. This approach allows for OSFI and FRFIs to collaborate in proactively identifying realistic cyber threats and better prepare with remedial actions. This in turn enhances the FRFI's prevention, detection, and response capabilities and by design, the stability and security of the broader financial sector in Canada.

2. Introduction

2.1 Purpose

The purpose of this document is to outline the methodology and process to follow when conducting an I-CRT assessment. This includes details on roles and responsibilities of stakeholders, key phases, activities, and deliverables as well as interactions associated with an I-CRT assessment.



Text description - Figure 1 - Intelligence-led Cyber Resilience Testing (I-CRT)

Intelligence-led Cyber Resilience Testing encompasses a Regular I-CRT Assessment process. This process is continuously performed by Intelligence and Ethical Hacking independent service providers, within the domain of the Internet, Third-Party Services, Gateway and on-premise environments. This type of testing helps advance the goals of cyber resiliency and a more cyber-resilient financial sector and institutions within it.

As shown in Figure 1, the overall objective of the I-CRT assessment is to regularly evaluate a FRFI's cyber-resilience posture by identifying cyber threats and associated possible remedial actions. The I-CRT assessment mimics the behaviors of sophisticated threat actors as assessed by commercial cyber intelligence and red team service providers. The I-CRT assessment is conducted in a controlled way and entails implementing a risk management

process to identify, assess, and mitigate risks related to I-CRT activity during all phases of the exercise.

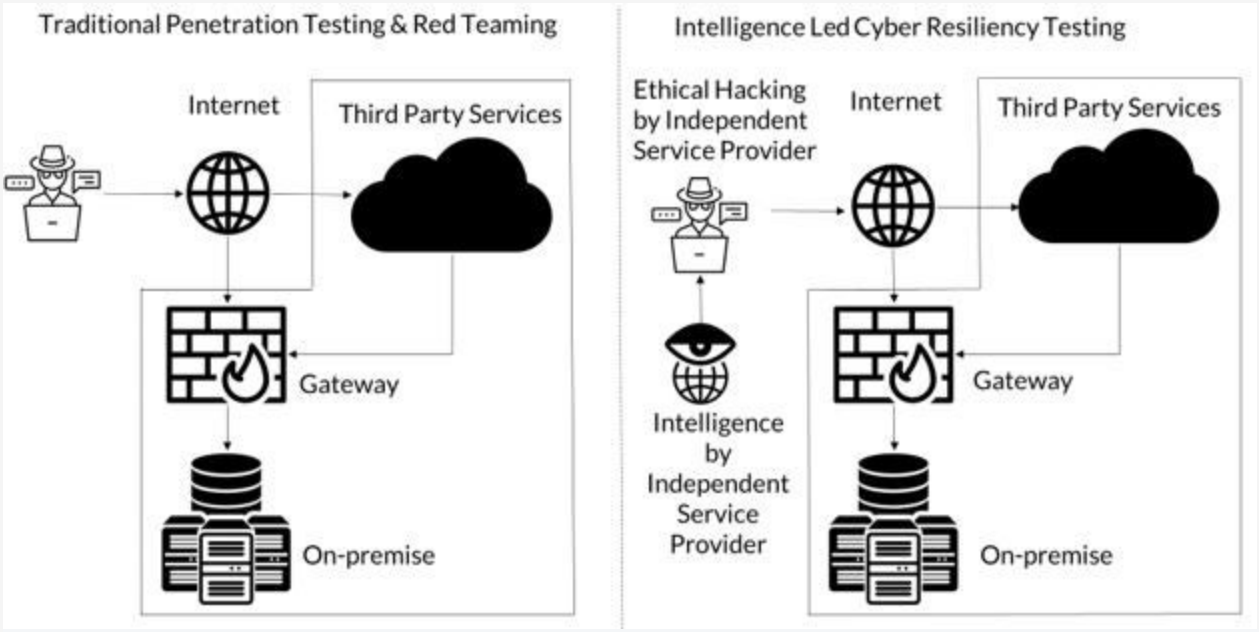
This document should be read with other relevant I-CRT documents referenced in Annex D – List of additional artifacts.

2.2 I-CRT

2.2.1 What is I-CRT?

Intelligence-led cyber resilience testing is a controlled-threat assessment of FRFI's cyber resilience. It leverages targeted threat intelligence (see Section 2.2.3) and simulates the advanced tactics, techniques, and procedures used by a sophisticated threat actor. The inclusion of targeted threat intelligence ensures the I-CRT assessment remains relevant and provides specific, timely, and actionable information. While the scope of the assessment is defined jointly by OSFI and the FRFI undergoing the testing, the risk management process is the responsibility of the FRFI's control group. As a prudential regulator, OSFI provides independent oversight and guidance throughout an I-CRT assessment. The details of roles and responsibilities are described in Section 3.1 of this document.

An I-CRT assessment evaluates a FRFI's cyber resilience (see Figure 1) including its existing controls, prevention measures, and detection capabilities. Simply stated, an I-CRT assessment identifies gaps or weaknesses that may affect cyber resilience. The FRFI in turn can take informed remedial actions in line with its business objectives and risk appetite.



Text description - Figure 2 - Traditional penetration testing/Red teaming vs. I-CRT

Intelligence-led Cyber Resilience Testing encompasses a Regular I-CRT Assessment process. This process is continuously performed by Intelligence and Ethical Hacking independent service providers, within the domain of the Internet, Third-Party Services, Gateway and on-premise environments. This type of testing helps advance the goals of cyber resiliency and a more cyber-resilient financial sector and institutions within it.

2.2.2 Penetration testing vs. Red teaming vs. I-CRT

Although traditional penetration testing, red teaming, and threat intelligence-led tests have a common goal of protecting systems and data from threat actors, they differ in many ways. As depicted in Figure 2, the underlying principle of I-CRT is that FRFIs will be subjected to a threat assessment on their live CBFs by independent service providers. With I-CRT, an ethical hacker, namely penetration tester or red-team tester is provided with threat intelligence targeted towards the CBFs as opposed to the traditional penetration testing and red teaming. The intelligence collected and utilized is from an independent source, i.e., a commercial vendor. Furthermore, the red teaming actions by the ethical hackers will themselves be independent from the FRFI and sourced from a commercial vendor.

Notable differences between traditional penetration testing compared to red teaming and threat intelligence-led testing are summarized in Table 1 below.

Table 1: Traditional penetration testing vs. Red teaming vs I-CRT

	Traditional penetration testing	Red teaming	Intelligence-led Cyber Resilience Testing
Mindset	Finding known vulnerabilities with standard tool set	Objective-based assessment aiming at persistent access to specific systems or information with a simulated attack	Aiming at persistent access to specific systems or information based on realistic threat scenarios
Scope	Technology-focused (web, network, hardware, applications etc.)	Testing scope goes beyond technology that is People, Process, Technology (PPT)	Testing scope goes beyond technology that is PPT associated with CBFs
Testing technique	Known technique (e.g., Top 10 industry standard vulnerability test cheat sheet)	Emulate sophisticated threat actors' Tactics, Techniques, Procedures (TTPs)	Identify CBF targets and emulate sophisticated threat actors' TTPs based on genuine cyber threats
Goal	Identifying as many vulnerabilities as possible	Identifying gaps not only in technology controls but also in processes and procedures	Identifying genuine cyber threats and vulnerabilities disrupting CBFs

From left to right in Table 1, as test type sophistication increases progressively the differentiating factor on the left becomes an inherent property of the testing approach on the right. Traditional penetration testing is an attempt to "exploit" an application or break into a network to identify as many vulnerabilities or design flaws as possible before they can be exploited by threat actors.

Red teaming takes the concept of penetration testing to the next level by using a war-gaming format that consists of two teams. The red team attempts to break into a network, moving laterally to avoid detection and eventually executing invasive actions, such as simulated data corruption, disruption and exfiltration. The red team usually employs tools, techniques, and procedures readily available via open source along with advanced and custom-built procedures and scripts to exploit vulnerabilities; it is an effective way to test and evaluate an organization's ability to detect and respond to a cyber-attack.

The defenders (aka blue team) attempt to detect and respond to the intrusion. To simulate a real-world event, the blue team is not advised ahead of time of a red teaming activity.

I-CRT is a natural evolution of red teaming reflecting targeted threat intelligence coupled with cutting edge cyber technologies. Sophisticated threat actors, for example, those who are state-sponsored or have links to organized crime, are well financed and employ cutting edge technology. To emulate the sophisticated threat actor, the concept of intelligence-led penetration testing was developed by the Bank of England with its CBEST framework and it has since been leveraged globally by regulators (e.g., TIBER, CORIE).

OSFI's I-CRT is Canada's approach to intelligence-led cyber resilience testing in the financial sector and it is influenced by these frameworks. Combining targeted threat intelligence and advanced tools, techniques, and procedures will result in synergies that closely mirror a sophisticated threat actor.

2.2.3 Targeted threat intelligence

Targeted threat intelligence is a set of genuine and realistic threat scenarios which can potentially disrupt a FRFI's CBFs and therefore forms the basis of the I-CRT assessment. A threat scenario describes a FRFI's actual target systems and their vulnerabilities. As technology landscape change, attack surfaces of a CBF may also evolve depending on a FRFI's existing controls, processes, procedures and their effectiveness. For threat scenarios to be genuine and realistic, the threat intelligence needs to consider FRFIs' evolving attack surfaces. Such intelligence may not be readily available from open sources and instead could be provided by a highly skilled commercial vendor that specializes in cyber threat intelligence. Targeted threat intelligence information should be:

- Tailored and targeted to the financial sector, the target FRFI and its CBFs;
- Strategic, operational and as well as actionable for an I-CRT assessment;
- Attributable to the TTPs from organized crime, nation states, and state-sponsored entities (e.g., sophisticated threat actors); and
- Used to derive a prioritized list of vulnerable assets and systems, possibly grouped with associated TTPs. This list can be used to combine relevant TTPs when red teaming in the Execution phase (see Section 5.3).

2.2.4 Advanced tools, techniques and procedures

To demonstrate an appropriate level of assurance that a FRFI's critical assets and services are protected against highly competent, resourced, and persistent threat actors, the level and sophistication of red team testing should be informed by the targeted threat intelligence. By leveraging the targeted threat intelligence, a red team tester employs advanced TTPs to simulate potential cyber-attacks by either malicious outsiders or insiders on the FRFI's CBFs.

2.2.5 CBFs in I-CRT scope

An I-CRT assessment scope is defined by the CBFs associated with a target FRFI. CBFs are described as follows:

The PPT[1] required to deliver a critical operation[2] which, if disrupted, could have an impact on the financial stability of a company and its resilience, safety, soundness, customer base, or market conduct. Financial institutions across the financial sector support and deliver these functions in different ways through their own internal processes, which are in turn supported by critical systems. These critical systems, processes, and the people surrounding them are the focus of a FRFI's threat intelligence and red teaming.

2.2.6 I-CRT assessment criteria and cadence

With increasing number of national and international cyber incidents in the financial sector, the threat landscape for FRFIs and TTPs is evolving rapidly. For continuous assurance on cyber resilience, I-CRT assessments should be conducted regularly. While I-CRT concepts in general apply to all FRFIs, the current scope of the I-CRT framework applies to all Systemically Important Banks (SIBs) and Internationally Active Insurance Groups (IAIGs). OSFI's recommendation as to when an I-CRT should be carried out is summarized in Table 2 below: I-CRT assessment criteria and cadence.

Table 2: I-CRT assessment criteria and cadence

Target FRFI	Triggers	Cadence
SIB & IAIG	Supervisory cycle	Three years
SIB & IAIG	FRFIs' technology & cyber risk potentially threatening financial stability Major cyber incidents impacting FRFIs' operational resilience	Event driven
Other FRFIs	FRFIs outside of SIBs and IAIGs may request an I-CRT assessment and OSFI will evaluate the request on a case-by-case basis.	Case by case

OSFI will review the I-CRT assessment and cadence requirements at a regular interval within its supervisory cycle and update if necessary.

3. Roles and responsibilities

The success of an I-CRT assessment is dependent on careful coordination and close collaboration of all stakeholders. The governance, planning, risk management, and execution of an I-CRT assessment is assigned to the following stakeholders:

- FRFI and FRFI Control Group (CG);
- Control Group Coordinator (CGC);
- Regulator (i.e., OSFI);
- Threat Intelligence service Provider (TIP); and
- Red Team service Provider (RTP).

3.1 FRFI and FRFI Control Group (CG)

The FRFI is represented by a senior executive sponsoring the I-CRT assessment. The FRFI then establishes a CG which takes the overall responsibility for conducting the I-CRT assessment. The CG consists of senior staff handling

security incident response and the relevant escalation chain. The CG should adhere to the following guidelines:

- Members should have relevant decision-making authority;
- The number of members should be as limited as possible, and information sharing within and beyond the group is only on a "need to know" basis; and
- To implement the I-CRT, members should provide essential information and knowledge about CBFs, business, IT and security process etc.

The CG has the overall responsibility for conducting the I-CRT assessment including the end-to-end project management, risk management, contracting of third-party suppliers, scoping, and remediation activities after the assessment. The CG has responsibility to:

- Assign an overall coordinator/lead for the I-CRT assessment;
- Create a project management plan and risk assessment document;
- Ensure the I-CRT assessment is conducted in a controlled manner by identifying, assessing, and mitigating risks throughout the assessment;
- Identify and communicate in a timely manner material issues to OSFI. For example, breach of operational secrecy (see Section 4.3) of the I-CRT assessment or a suspected compromise of the assessment;
- Contract, fund, and manage TIP and RTP;
- Coordinate and communicate with OSFI, TIP, and RTP; and
- Ensure deliverables are produced in accordance with I-CRT guidelines and shared with OSFI in a timely manner.

A fulsome list of responsibilities of both the FRFI and the CG are in Annex C – I-CRT RACI.

3.2 Control Group Coordinator (CGC)

The CGC is responsible for coordinating all CG activities mentioned in Section 1.1, including the quality assurance and project management of I-CRT. The CGC ensures all I-CRT stakeholders collaborate and perform their tasks appropriately and provides regular status updates to FRFI executives and other stakeholders as required. The CGC should solicit OSFI's approval for any changes to the CG membership.

3.3 Regulator

As the regulator, OSFI provides oversight and guidance throughout the I-CRT assessment to ensure it is conducted in accordance with the I-CRT framework. OSFI is responsible for selecting a FRFI for an I-CRT assessment based on assessment criteria (see Section 2.2.6).

OSFI teams comprise relevant supervision staff and cyber specialists to oversee a FRFI's execution of an I-CRT assessment.

More specifically, OSFI:

- Evaluates the I-CRT assessment criteria for a FRFI and initiates an I-CRT for a target FRFI if requirement is met;
- Provides end-to-end oversight of the I-CRT assessment at all phases (e.g., initiation, threat intelligence, execution, and closure);
- Participates with the CG to define and agree on the I-CRT scope;
- Provides feedback on the selection of the TIP and the RTP;
- Reviews the findings and remediation plan from the I-CRT assessment and issues a letter with recommendations to ensure findings are tracked and addressed in a timely manner;
- Leverages the results of the I-CRT assessment for thematic sector analyses of vulnerabilities; and
- Monitors the remediation actions on any findings by leveraging OSFI standard Supervision process until issue closure.

A fulsome list of all OSFI's responsibilities is included in the Responsible, Accountable, Consulted and Informed (RACI) matrix defined in Annex C – I-CRT RACI.

3.4 Threat Intelligence service Provider (TIP)

The TIP is a commercial company that specializes in providing targeted threat intelligence and services. The TIP possesses significant experience in researching cyber threats and providing threat assessments, covering areas such as:

- Cyber threats to financial institutions;

- Threat actors (e.g., nation state, organized cyber criminals); and
- Advanced tools techniques and procedures.

The TIP is contracted by the CG to perform the following tasks:

- Provide a cyber threat intelligence assessment of the FRFI including evidentially supported profiles of cyber threat actors that could potentially target the FRFI;
- Provide information that potential threat actors could uncover regarding CBFs or related functions or systems;
- Create threat scenarios based on the outcomes of the targeting assessment and threat intelligence;
- If required, provide additional intelligence and consultations during the I-CRT execution phase and input to the final report;
- Participate in the playback/walkthrough of the red team activities and threat scenarios with the FRFI, OSFI, and RTP; and
- Provide feedback on the FRFI threat intelligence gathering capability.

A fulsome list of the responsibilities of TIP is included in the RACI of Annex C – I-CRT RACI.

3.5 Red Team service Provider (RTP)

The RTP is a commercial company that specializes in conducting red teaming activities. The RTP leverages the threat scenarios provided by the TIP to build a red team testing plan.

The RTP is required to complete the following tasks:

- Based on the threat scenarios and threat models provided by the TIP, design and develop a Red Team Test (RTT) plan targeting the CBFs and systems;
- Work closely with the CG to create a RTT risk management plan to manage the risks of conducting red teaming on live systems;
- Execute the RTT plan using an ethical red teaming methodology;
- Provide regular updates to CG during the red teaming assessment;

- Provide a report to the FRFI detailing the red teaming assessment results including exploits, targets in the scope that were attained, and targets in the scope that were not attained;
- Provide a report to OSFI, summarizing the red teaming assessment results excluding FRFI specific confidential and sensitive information; and
- Provide feedback on the FRFI incident detection and response capability.

A fulsome list of all responsibilities of the RTP is included in the RACI of Annex C – I-CRT RACI.

3.6 Role of other regulators

It is recognized that FRFIs often have global/multi-jurisdictional operations and thus are also subject to regulation from other jurisdictions (e.g., foreign and provincial). When a FRFI is undergoing an I-CRT assessment where in-scope assets are located in other jurisdictions, OSFI will inform the relevant regulatory authorities for their awareness. OSFI will work with the FRFI to ensure that there is no overlap of scope with similar assessments done in foreign jurisdictions by other regulatory bodies. OSFI will not disclose confidential FRFI information.

4. Risk management

Managing the risk of an I-CRT assessment is critical to the success of the assessment and aims to keep the CG in control of the I-CRT during all its phases.

I-CRT phases

1. Initiation
2. Threat intelligence
3. Execution
4. Closure

Continuous risk assessment is done through all phases

4.1 I-CRT risk owner

The FRFI's CG is responsible for executing the I-CRT risk assessment in a controlled manner. This also includes mitigating the identified risks continuously throughout the I-CRT assessment as indicated. In particular, the CG should conduct an initial risk assessment and identify measures to mitigate any risks as necessary. The management of risks should be a continuous process throughout the I-CRT assessment.

4.2 Risk considerations

The highest risks in terms of potential disruption to FRFI activities occur during the red-teaming phase, a.k.a. the execution phase in the I-CRT assessment. Red teaming of operational systems or CBFs will always possess a level of inherent risk. The CG remains in control for the I-CRT assessment and at any time may order the cessation of red team activities should there be concerns.

The CG should assess and manage risks covering both strategic and operational aspects of all activities. These include, but are not limited to:

- Scope of the I-CRT;
- Escalation procedures;
- Confidentiality of the I-CRT assessment and "need to know" principle;
- Targeting of CBFs/systems;
- Project timing/scheduling;
- Contracting of third-party service providers; and
- Execution of third-party activities.

4.3 Operational secrecy

To ensure the success of an I-CRT assessment, strict operational secrecy is required throughout the exercise. As mentioned before in section 3.2, if the secrecy is compromised or suspected to be compromised, the CGC should immediately report it to OSFI. Adopting the "need to know" principle, only selected individuals should be aware that an I-CRT assessment is being planned. This includes but is not limited to the blue team. If the blue team is aware of

an I-CRT assessment, this severely impacts the efficacy of the I-CRT assessment as the pre-knowledge or awareness of potential anomalies or alerts will not fully assess the blue team's ability to respond to a sophisticated cyber attack.

To further enhance operational security, a project code name is assigned for the assessment and the Traffic Light Protocol (TLP) for information sharing to apply. Additional information on the TLP can be found in Annex B – Traffic Light Protocol (TLP).

4.4 Independent service providers

To achieve targeted threat intelligence for a given scope and to ensure a successful red teaming execution, it is very important that the activities for threat intelligence gathering and red teaming are sufficiently separate and distinct. The immediate benefits of having two separate vendors to conduct the threat intelligence gathering and the red teaming include independence and different types of knowledge. While both service providers need to work together in some cases (see Annex C – I-CRT RACI for details), their independence reduces the risk of influence with conscious or unconscious biases.

From an I-CRT perspective, it is recommended to contract separate vendors for the threat intelligence and the red teaming. Prior to selecting vendors, due diligence is required on the part of the FRFI to ensure that the vendors possess the requisite skills set, experience, and capability to obtain, synthesize, and produce targeted threat intelligence and red teaming. It is insufficient to simply conduct an Internet or dark web search of known cyber actors and their tools.

Where a FRFI may wish to have one service provider for both threat intelligence and red teaming, an assessment should be conducted beforehand to identify risks and compensating controls. OSFI reviews the assessment and provide feedback. An over-riding stipulation is that there should be a separation between the two activities and no information or communication should be shared between the service providers unless required for greater collaboration and better intelligence and red teaming actions.

5. I-CRT process

The I-CRT process is divided into four phases. This indicative timeframe should not be used as a predefined duration. A rule of thumb is to allocate adequate time for each phase based on the I-CRT scope. Each phase is further described in the subsequent sections. The activities producing deliverables are also listed accordingly.

Duration for I-CRT phases

1. Initiation (6-8 weeks)
2. Threat Intelligence (6-10 weeks)
3. Execution (8-12 weeks)
4. Closure (4-6 weeks)

5.1 Initiation phase

The initiation phase formally launches the I-CRT activity. OSFI formally engages the FRFI, the I-CRT assessment scope is established, and service providers are selected and onboarded by the FRFI. The duration of the initiation phase largely depends on the FRFI's procurement process. As shown in the duration for I-CRT phases, this phase should take approximately 6-8 weeks to complete.

Initiation phase

1. Launch
2. Engagement
3. Scoping
4. Procurement

Procurement can occur in conjunction with scoping, but scoping must be completed before the procurement phase is completed.

5.1.1 Launch

As depicted in the initiation phase, the launch marks the start of the I-CRT initiation phase. Upon selection of a FRFI for an I-CRT assessment, OSFI issues a formal letter to notify the FRFI that it has been selected for an I-CRT. The letter also includes a description of the I-CRT objective, scope, approach, and reporting.

The output of this activity is an I-CRT letter by OSFI.

5.1.2 Engagement

Upon receipt of the OSFI's I-CRT letter, the FRFI identifies the potential CG members and establishes the CG and CGC, ensuring they are aware of their roles and responsibilities.

OSFI conducts a kickoff meeting with the FRFI where the following topics are discussed:

- I-CRT process;
- I-CRT stakeholders and their roles and responsibilities;
- Third party service provider contractual considerations; and
- I-CRT project schedule and risk management.

The CG then takes the lead by creating a project management plan that outlines the assessment activities. To identify risks and appropriate measures, the CG also creates a risk management plan.

The outputs of this activity are:

- I-CRT project management plan by CG; and
- I-CRT risk assessment document by CG.

5.1.3 Scoping

The FRFI and OSFI collaborate and agree on a scope for the I-CRT activity, culminating in a scope specification document to be used as an input for the procurement phase.

OSFI provides an I-CRT scoping template to CG and facilitates a workshop with the CG to discuss the FRFI's CBFs and complete the scoping exercise. As a result of the workshop, a list of key systems and services underpinning each of

the scoped CBFs is documented in the I-CRT Scope Specification. Both parties should agree on the scope before proceeding further. Any changes to the agreed scope should be discussed with OSFI.

The output of this activity is the I-CRT scope specification by the CG.

5.1.4 Procurement

The FRFI may initiate a procurement process concurrently with the I-CRT scoping exercise. The scope of an I-CRT assessment should be completed before selecting vendors. As shown in the initiation phase, vendor selection and onboarding cannot be finalized if the scoping is not agreed on and finalized by OSFI and the CG.

The FRFI is responsible for the selection, contracting, and payment of the TIP and the RTP. OSFI may provide feedback on the selection of the providers, however, the FRFI is responsible for all aspects of the procurement process.

5.2. Threat Intelligence phase

The objective of the threat intelligence phase is to determine realistic cyber threat scenarios (i.e., cyber threat profile) of the FRFI against the scope established in the initiation phase. This phase is critical as it lays the groundwork for the execution phase, where the actual red teaming activities occur. To achieve a realistic cyber threat profile, the TIP first receives direction from the CG. The TIP proceeds with the threat intelligence gathering and creation of the Threat Intelligence Report. The TIP should also provide its assessment on the FRFI threat intelligence capability.

Threat intelligence phase

1. Direction
2. Intelligence
3. Review
4. Assessment

5.2.1 Direction

The CG will share the scoping document with the TIP and the RTP. The CG decides whether FRFI information such as business and technical documentation of systems, prior threat assessment results, and recent relevant incidents should be provided to the TIP. The TIP may then consider this information when developing the threat intelligence plan that should be focused on the FRFI's CBFs.

The output of this activity is the threat intelligence plan by the TIP.

5.2.2 Intelligence

Based on the threat intelligence plan, the TIP collects, analyzes, reviews, and consolidates relevant threat information for a period of time. The TIP consolidates threat information from different sources, including the FRFI's own threat intelligence, in a structured manner resulting in a formal FRFI cyber threat profile for the I-CRT assessment. As described in Section 2.2.3, the threat information can range from a very high-level description of technology and cyber vulnerabilities, including threat actors, their TTPs and threat vectors to indicators of compromises (IoCs) related to CBFs.

Upon completion of the above activities, the TIP develops threat scenarios describing malicious threat actor behaviors and their impact on the target functions. Such scenarios are then mapped to one or more CBFs. These are essentially a cyber threat profile of the FRFI's CBF. The TIP then uses the developed cyber threat profile information to produce the threat intelligence report. The description in the report is essentially the cyber threat profile of scenarios including, but not limited to:

- Objective and target of the attack;
- Information about the threat actors and their intent; and
- TTPs.

The CGC disseminates the threat intelligence report to relevant stakeholders (e.g., RTP, OSFI) for their information. As the threat intelligence report is available at this stage, the RTP can start drafting an initial RTT plan.

The outputs of this activity are:

- Initial threat intelligence report by TIP; and
- Initial RTT plan by RTP.

5.2.3 Review

Once the initial threat intelligence report is produced, it is shared with the relevant stakeholders (e.g., CG, RTP, OSFI) for review and feedback. OSFI runs a workshop with the FRFI, TIP and RTP to ensure that the threat profile is realistic and indicative of the CBFs in scope. Following the workshop, the TIP consolidates post workshop actions and produces the final version of the threat intelligence report. The threat intelligence report is reviewed by OSFI and then approved/accepted by the CG.

The RTP may need to revise the initial draft RTT plan in light of the workshop and the risks identified. Finally, the CG reviews the I-CRT project plan and risk assessment based on the workshop. The CGC ensures key stakeholders are aware of any changes related to identified risks and measures in the I-CRT assessment.

The outputs of this activity are:

- Final threat intelligence report by TIP;
- Revised RTT plan by RTP;
- Revised I-CRT project plan by CG; and
- Revised risk assessment by CG.

5.2.4 Assessment

The assessment is the final activity conducted during the threat intelligence phase. In this activity, the TIP provides its opinion on the FRFI's internal threat intelligence capability.

5.3 Execution

Once the FRFI cyber threat profile is finalized in the threat intelligence phase, the RTP takes over. During the execution phase, the subject matter experts of the RTP take the role of potential threat actors and conduct the actual invasive activities (i.e., red teaming) against the FRFI assets associated with the CBFs in scope. Prior to the commencement of the execution phase, OSFI may inform the Canadian Center for Cyber Security (CCCS) for their

awareness.

With the goal of a comprehensive assessment, adequate time should be reserved for the execution of the RTT plan. While the duration of the execution phase depends on many factors, such as scope, resources etc., experience to date indicates that the maximum period of the I-CRT assessment time is spent in the execution phase (see duration for I-CRT phases). It is important to reiterate that preserving operational secrecy (as described in Section 4.3) during the entire execution phase is key to achieving a credible overview of the FRFI's cyber resiliency. The results of the RTT are documented in appropriate reports. As part of execution, the RTP should opine on the FRFI's incident detection and response capability.

Execution phase

1. Planning
2. Red Teaming
3. Review
4. Assessment

5.3.1 Planning

As the RTP is already aware of the I-CRT scope and also has access to the threat intelligence report, it is able to finalize the initial draft of the RTT plan created during the threat intelligence phase. To this effect, for each scenario of the threat intelligence report, the RTP develops RTT scenarios as part of the RTT plan that include detailed steps, advanced tools, techniques, and procedures. The final RTT plan should describe how a scenario ultimately addresses:

- The threat scenarios described by the TIP in the threat intelligence report; and
- The CBFs in the I-CRT scope specification.

Conducting any kind of red teaming activities always involves a level of risk to the CBFs. Risks to the FRFI, such as degradation or outage of service or disclosure of sensitive information, needs to be kept to an absolute minimum. The CG, working with the RTP, should therefore include an appropriate plan for managing this risk. The CG should

review and approve the RTT plan and the risk assessment before proceeding further.

The outputs of this activity are:

- Final RTT plan by the RTP; and
- The RTT risk management plan by the CG and RTP.

5.3.2 Red teaming

Following the completion of the planning phase, the RTP executes an I-CRT against the target assets and services (i.e., CBFs) determined during scoping (see Section 5.1.3). The red team, as it progresses through the RTT plan, should attempt to achieve threat actor goals identified during the threat intelligence phase (see Section 5.2).

The RTP, like the TIP, is constrained by available time and resources as well as moral, ethical and legal boundaries. It is therefore possible that the RTP and the FRFI could discuss a potential 'de-chaining' in the event of slow progress in the assessment. Any such activity should be agreed upon with OSFI. A 'de-chaining' activity involves the RTP being given some assistance to move to the next phase of the attack to test vulnerabilities that the RTP may otherwise not have sufficient time to test.

The results of the red team activities provide information on critical vulnerabilities and may also include weaknesses/gaps in controls, processes, and procedures. The results should also include recommendations from the RTP. To capture the results on a 'need to know' basis, the RTP produces two different RTT reports, one for the FRFI and the other for OSFI. While both reports contain description of the results in relation to the threat scenarios and relevant tests, the report for OSFI must not contain any confidential or sensitive information (such as personally identifiable information and technical details, e.g., IP address, system names, emails, configuration details, etc.).

The outputs of this activity are:

- Initial RTT report for the FRFI by the RTP; and
- Initial RTT report for OSFI by the RTP.

5.3.3 Review

The CG, OSFI, RTP and TIP hold a workshop to review the outcomes of the red team test as detailed in the draft Red Team Test Report. The workshop is arranged by OSFI to discuss:

- RTT execution performance and identified vulnerabilities (led by the RTP); and
- Mitigating factors and proposed remediation (led by the CG).

Based on the discussions at the workshop, the RTT reports will be finalized by the RTP.

After the review workshop, the CG should start working on a draft remediation plan considering the vulnerabilities and recommendations identified as a result of the RTT.

The outputs of this activity are:

- Final RTT report for the FRFI by the RTP;
- Final RTT report for OSFI by the RTP; and
- Initial remediation plan by the CG.

5.3.4 Assessment

This is the final activity of the execution phase. In this activity, RTP provides its opinion on the FRFI's incident detection and response capability.

5.4 Closure phase

Upon completion of the execution phase, the I-CRT assessment enters the closure phase. In this phase, the FRFI finalizes the remediation plan and OSFI issues a supervisory letter that captures a summary of findings with recommendations to the FRFI. OSFI expects formal responses with remediation plans for any findings, and these will be monitored and tracked as part of the regular supervisory process.

Closure phase

1. Remediation
2. Supervision

5.4.1 Remediation

Critical to learning, all stakeholders participate in a debrief of the red team activities including a review of the cyber threat assessment conducted by the TIP and RTP.

Using a risk-based approach, the CG finalizes the draft remediation plan developed in the I-CRT execution phase.

Similar to any other supervisory work, OSFI analyzes the facts (i.e., RTT report) along with its own observations throughout the I-CRT assessment. Based on this analysis and review, OSFI findings and recommendations are finalized and shared with the FRFI in a wrap-up meeting. OSFI will then issue a supervisory letter to the FRFI summarizing the findings and recommendations. The FRFI should provide detailed action plans to remediate findings noted in the OSFI letter. OSFI will leverage the results of the I-CRT assessment for thematic sector analyses of vulnerabilities.

In its letter, OSFI may provide an "I-CRT Label" to attest that the FRFI has undergone an I-CRT assessment that is consistent with the requirements of the I-CRT framework. OSFI reserves the right to not label an I-CRT assessment if the FRFI does not strictly follow the requirements of the framework.

The output of this activity is an OSFI supervisory letter.

5.4.2 Supervision

Following the issuance of the OSFI supervisory letter, OSFI monitors the FRFI's remediation activities until the closure of all findings. The findings and recommendations issued in the supervisory letter will be treated as those from a supervisory review and will require evidence to support closure.

6. Legal disclaimer

The information and concepts presented in this document are for information purposes only. The I-CRT framework does not constitute legal and/or other professional advice and the information should not be relied on or treated as

a substitute for specific advice relevant to particular circumstances. OSFI accept no responsibility for any errors, omissions or misinterpreted statements in this document, or for any loss that may be caused from reliance on the information and concepts presented within it.

7. Annex A – Glossary

CBF

Critical Business Function (CBF) sets out the scope of an I-CRT assessment. CBFs are described as the people, processes and technology required to deliver critical operations[2] which, if disrupted, could have an impact on the financial stability of a company and its resilience, safety, soundness, customer base, or market conduct. Financial institutions across the financial sector support and deliver these functions in different ways through their own internal processes, which are in turn supported by critical systems. These critical systems, processes, and the people surrounding them are the focus of a FRFI's threat intelligence and red teaming.

CGC

Control Group Coordinator - The CGC is responsible for overall coordination for the FRFI

CG

Control Group - The CG is responsible for the management of the I-CRT assessment

CORIE

Cyber Operational Resilience Intelligence-led Exercises

CBEST

Cyber resilience framework by the Bank of England/Prudential Regulatory Authority

FRFI

Federally Regulated Financial Institutions

Intelligence-led Cyber Resilience Testing (I-CRT)

This is a test of an organization's resilience to detect, respond and withstand a cyber-attack. It is different from a red team exercise or penetration testing as an independent third party provides realistic threat scenarios against CBFs which then inform another independent third party that mimics the sophisticated threat actors, and the cyber-attacks using specially crafted tools, techniques and procedures.

RTP

Red Teaming service Provider (RTP) is responsible for the red teaming activities performed in the execution phase

RTT

Red Teaming Test activities by RTP

TIBER

Threat Intelligence-Based Ethical Red Teaming

TIP

Threat Intelligence service Provider (TIP) is responsible for the threat intelligence phase

8. Annex B – Traffic Light Protocol (TLP)

Operational secrecy and the adherence to the "need to know" principle are essential to the success of I-CRT. Information must be safeguarded and shared on a need-to-know basis. The following provides guidance for information handling.

Purpose and background

OSFI recognizes that effective, cohesive, and coordinated communication is integral to the success of Project **NAME** (The Project).

The purpose of this document is to describe an overarching approach for effectively communicating information throughout the project lifecycle.

Information handling

Information confidentiality, completeness and accuracy is an important asset in Project **NAME** and a critical factor in the successful outcome of the Project. In addition to maintaining the security of sensitive information created as part of this project, ensuring its integrity is equally important.

To allow for consistent handling of project-related information, all documents must be labeled as appropriate.

Traffic Light Protocol (TLP)

This Traffic Light Protocol (TLP)[3] has been developed to facilitate sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs three (3) colours to designate expected sharing boundaries to be applied by the recipient(s).

Project **NAME** TLP only has three colours; any designations not listed in this document are not considered valid. All project documents, including email, should include the appropriate TLP label. If a recipient believes the information requires broader distribution than indicated by the original TLP designation, they must obtain explicit permission from the original source.

General usage: when affixing a label to a document, please ensure to use capital letters with the designated colour bolded.

Note, however, these labels are not intended to supersede confidentiality statements or non-disclosure agreements.

Project NAME: TLP

Colour	How it can be shared	Example(s)
TLP: **RED** Not for disclosure, for recipient(s) only	Recipients **may not** share TLP: **RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.	TLP: **RED** information is limited to those present at the meeting or recipient(s) of an email from the source.
TLP: **AMBER+STRICT** Limited disclosure, restricted to the members of the organization involved with Project **NAME**	Recipients may only share TLP: **AMBER+STRICT** information with members of their own organization directly involved with Project **NAME**. Information **cannot** be shared with vendors (e.g., TIP and RTP)	TLP: **AMBER+STRICT** information at a meeting can be shared only to those from the organization.
TLP: **AMBER** Limited disclosure, restricted to Project **NAME** participants within our respective organizations.	Recipients may only share TLP: **AMBER** information with members of their own organization directly involved with Project **NAME**, and with vendors (e.g., TIP and RTP) who **need to know** the information.	TLP: **AMBER** information at a meeting can be shared beyond those present, provided there is a bona fide need-to-know.
TLP: **GREEN** Limited disclosure, restricted to employees within our respective organizations.	Sources may use TLP: **GREEN** when information is useful for the awareness of all participating individuals/organizations as well as with peers within the broader community or sector. Recipients may share TLP: **GREEN** information with peers/colleagues within their organization, but not via publicly accessible channels.	TLP: **GREEN** Information in this category can be circulated widely within a particular community. Information may not be released outside of the community. (community defined as FRFI, OSFI and 3rd parties contracted for Project **NAME** work).

9. Annex C – I-CRT RACI

The roles and responsibilities for the stakeholders of an I-CRT assessment are listed using the following Responsible (R), Accountable (A), Consulted (C) and Informed (I) notions, also known as RACI matrix.

I-CRT RACI matrix for phase Initiation, by stakeholder

Sub-phase	Description	FRFI executive sponsor	CG	OSFI	TIP	RTP
Launch	I-CRT requirement assessment	-	-	R/A	-	-
	Issue Letter to FRFI	I	-	R/A	-	-
Engagement	I-CRT Control Group (CG) Identified and Established	A/R	-	C	-	-
	CG Coordinator (CGC) Identified and Assigned	A/R	R	C	-	-
	Engagement Workshop/Kick-off Meeting	A	C	R	-	-
	Create I-CRT Project Management Plan	A	R	I	-	-
	Create I-CRT Risk Assessment Document	A	R	I	-	-
Scoping	Create Scope Specification Document	A	R	C	-	-
	Coordinate Scoping Workshop	A	C	R	-	-
	Acceptance of Scope Document	A	R	R	-	-
Procurement	Initiate Procurement Process	R/A	C	I	-	-
	Define Vendor Selection Criteria	R/A	C	C	-	-
	Vendor Selection for TIP and RTP	A	R	C	I	I
	Onboard Vendors (TIP and RTP) and Confirms Readiness to Commence threat intelligence (TI) phase	A	R	C	C	C

I-CRT RACI matrix for phase Threat Intelligence, by stakeholder

Sub-phase	Description	FRFI executive sponsor	CG	OSFI	TIP	RTP
Direction	Share Scope Document With TIP and RTP	A	R	I	I	I
	Provide Relevant Information to TIP (e.g., business and technical overview of systems, current FRFI threat assessment, examples of recent attacks/incidents etc.)	A	R	I	C	-
	Review CBFs, Supporting Systems and Threat Assessment	A	C	I	R	-
	Produce the Threat Intelligence Plan	A	C	C	R	-
Intelligence	Execution of Threat Intelligence Assessment	A	C	I	R	I
	Creation of Threat Intelligence Report	A	C	C	R	I
	Commence Initial Draft Red Team Test (RTT) Plan	A	C	C	C	R
Review	Review Workshop	A	C	R	C	C
	Acceptance of Threat Intelligence Reports	A	R	C	I	I
	Regulatory Oversight of Threat Intelligence Reports	A	I	R	I	I
Assessment	Opine on FRFI Threat Intelligence Capability	A	C	I	R	-

I-CRT RACI matrix for phase Execution, by stakeholder

Sub-phase	Description	FRFI executive sponsor	CG	OSFI	TIP	RTP
Planning	Finalize of Red Team Test (RTT) Plan	A	C	C	I	R
	Creation of RTT Risk Assessment Document	A	R	C	I	R
	Acceptance of RTT Plan and Red Team Risk Assessment	A/R	R	I	I	I
Red Teaming	Red Team Execution	A	C	C	-	R
	Creation of a Red Team Test Report to FRFI (Detail and Technical Report to FRFI)	A	C	C	-	R
	Creation of a Red Team Test Report to OSFI (should not contain and confidential information)	A	C	C	-	R
Review	Review Workshop	A	C	R	C	C
	Acceptance of Red Team Test Report	A	R	C	I	I
	Regulatory oversight of Red Team Test Report	A	I	R	I	I
Assessment	Opine on FRFI Incident Detection and Response Capabilities	A	C	I	-	R

I-CRT RACI matrix for phase Closure, by stakeholder

Sub-phase	Description	FRFI executive sponsor	CG	OSFI	TIP	RTP
Remediation	Debrief of Red Team Activities Including Cyber Threat Scenarios	A	R	I	R	R
	Create Risk-based Remediation Plan	A	R	I	-	-
	Finalize Findings and Recommendation	I	I	R/A	-	-
	Conduct Wrap Up Meeting	C	C	R/A	-	-
	Issue Supervisory Letter	I	I	R/A	-	-
Supervision	Monitor Issues Until Closure	I	I	R/A	-	-

10. Annex D – List of additional artifacts

10.1 Templates

I-CRT templates set out expectations for relevant tasks in different I-CRT phases. The templates provides headers, topics and sections to capture and present information in a structured manner. The list below includes a set of I-CRT templates.

- I-CRT Scope Specification
- I-CRT Threat Intelligence Report Specification
- I-CRT Red Team Testing Report Specification

1 Which may include assets and services at third parties including public cloud.

2 Operational resilience key definitions

3 Based on Forum of Incident Response and Security Teams (FIRST)'s TLP model