# Préavis

| | |
|---|---|
| **Titre** | Cadre d'exécution du test de la cyberrésilience fondé sur le renseignement du BSIF |
| **Catégorie** | Saines pratiques commerciales et financières |
| **Date** | 1 avril 2023 |
| **Secteur** | Banques<br>Succursales de banques étrangères<br>Sociétés d'assurance vie et de secours mutuels<br>Sociétés d'assurance multirisque<br>Sociétés de fiducie et de prêts |

## Table des matières

Liste des figures



Liste des tableaux

## 1. Avant-propos

Le cyberrisque demeure un risque prépondérant pour bon nombre de secteurs, dont le secteur financier. Les cyberattaques peuvent perturber les fonctions opérationnelles essentielles (FOE) d'une institution financière fédérale (IFF) au point de menacer la viabilité de cette dernière, ou de se répercuter sur les consommateurs et les autres intervenants du marché dans le secteur financier. La gestion efficace du cyberrisque est un volet indispensable de la cyberrésilience d'une IFF. À titre d'outil de surveillance, le présent guide expose la marche à suivre au BSIF pour réaliser et évaluer les test de la cyberrésilience fondés sur le renseignement (TCFR). Il ne constitue pas un instrument de politique servant à établir les attentes sur le plan de la réglementation.

Les cyberattaques sont de plus en plus complexes, et leurs conséquences, de plus en plus graves, ce qui accentue la nécessité de mettre en place des mesures qui favorisent la résilience face aux cyberévénements et aux perturbations technologiques. Une façon efficace d'augmenter cette résilience consiste à adopter le point de vue de l'auteur d'une menace et à appliquer la méthode de test de l'équipe rouge en utilisant des renseignements de qualité afin de reproduire un contexte aussi réel que possible. Le TCFR est un test contrôlé et personnalisé fondé sur le renseignement, appliqué aux actifs et services technologiques sous-jacents d'une IFF à l'appui de ses FOE. Une évaluation du TCFR est une activité dirigée par l'organisme de réglementation (c.-à-d. le BSIF) où ce dernier fournit des consignes et exerce une supervision tout au long de l'exercice. Cette approche permet au BSIF et aux IFF de cerner ensemble et de façon proactive des cybermenaces réalistes et de mieux s'y préparer au moyen de mesures correctives. Cette façon de faire renforce les capacités de prévention, de détection et d'intervention des IFF et, par conséquent, la stabilité et la sécurité de l'ensemble du secteur financier au Canada.

# 2. Introduction

## 2.1. Objectif

Le présent document vise à décrire la méthodologie et la marche à suivre pour réaliser les évaluations du TCFR. Il comporte aussi des précisions sur les rôles et responsabilités des différents intervenants, les étapes, activités et livrables clés, de même que les interactions qu'implique une évaluation du TCFR.

La source média référencée est manquante et doit être réintégrée.

Description texte - Figure 1 – Test de la cyberrésilience fondé sur le renseignement (TCFR)

Les tests de la cyberrésilience fondés sur le renseignement doivent respecter le processus normal d'évaluation du TCFR. Il s'agit d'un processus en continu que suivent les fournisseurs de services indépendants de piratage éthique et de collecte de renseignements sur les menaces; ils doivent appliquer ce processus à la fois à Internet, à la passerelle et au réseau local. Ce type de test aide à faire progresser les objectifs de cyberrésilience et à accroître la résilience du secteur financier et des institutions financières.

Comme l'indique la figure 1, l'objectif général de l'évaluation du TCFR est d'évaluer périodiquement la posture de cyberrésilience d'une IFF en cernant les cybermenaces et en établissant les éventuelles mesures correctives requises. L'évaluation du TCFR imite les comportements des auteurs de menaces sophistiqués évalués par des fournisseurs privés de renseignements sur le cyberrisque et de services d'équipe rouge. L'évaluation du TCFR est menée de façon contrôlée et comprend la mise en place d'un processus de gestion du risque pour détecter, évaluer et atténuer les risques associés à un TCFR à toutes les étapes de l'exercice.

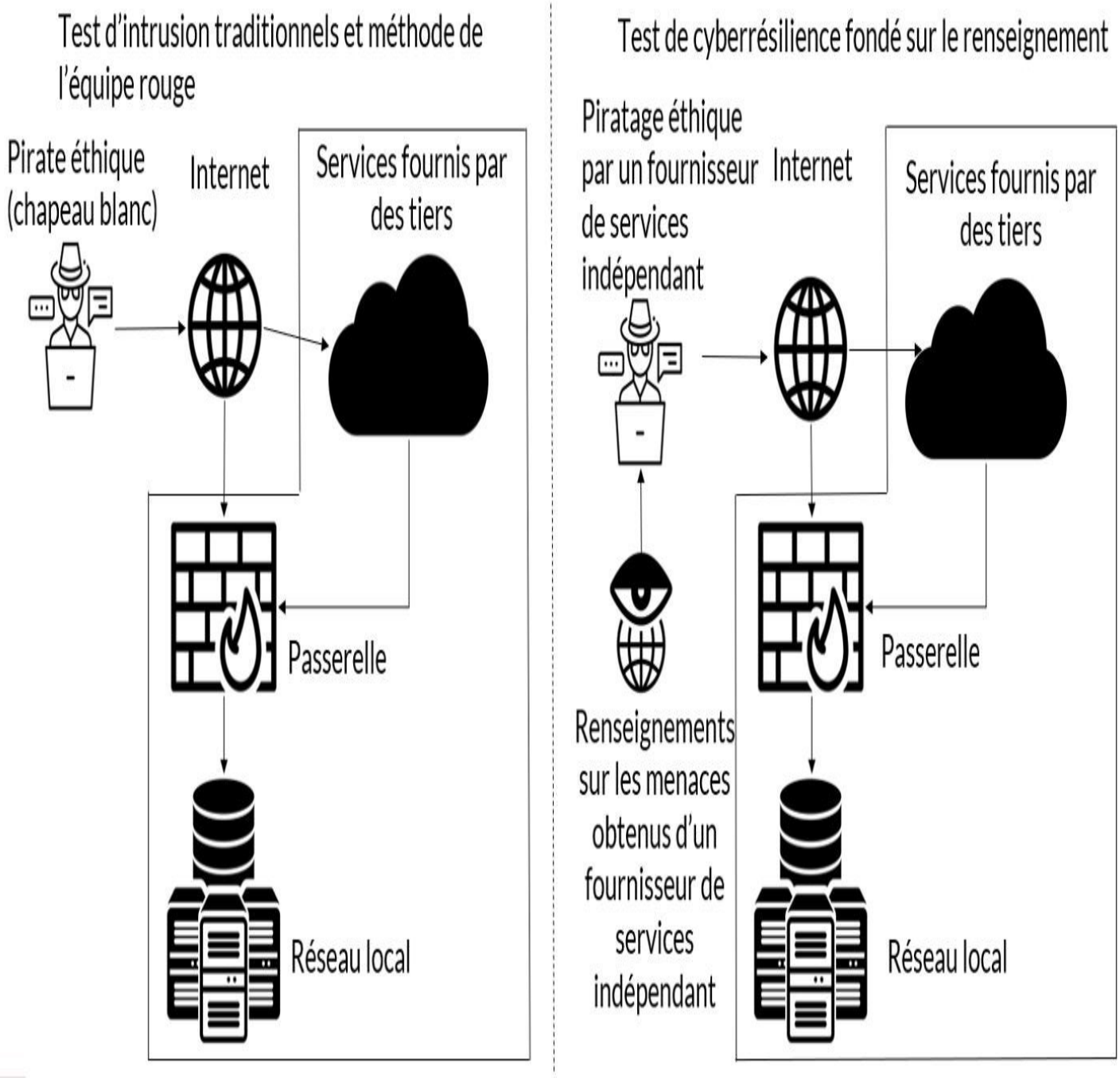
Le présent document doit être lu conjointement avec les autres documents pertinents mentionnés à l'annexe D, Outils supplémentaires.

## 2.2. Test de cyberrésilience fondé sur le renseignement (TCFR)

### 2.2.1. Définition du TCFR

Le test de la cyberrésilience fondé sur le renseignement est une évaluation contrôlée de la cyberrésilience d'une IFF en situation de menace. Il met à profit les renseignements sur les menaces ciblées (section 2.2.3) et simule les tactiques, les techniques et les procédures de pointe employées par un auteur de menaces sophistiqué. L'inclusion des renseignements sur les menaces ciblées fait en sorte que l'évaluation du TCFR demeure pertinente et fournit des renseignements précis, d'actualité et utilisables. Bien que la portée de l'évaluation soit définie conjointement par le BSIF et l'IFF visée par le test, le processus de gestion du risque relève du groupe de contrôle de l'IFF. En qualité d'organisme de réglementation prudentielle, le BSIF exerce une supervision indépendante et fournit des consignes tout au long de l'évaluation du TCFR. Les rôles et responsabilités sont décrits en détail à la section 3.1 du présent document.

Une évaluation du TCFR mesure la cyberrésilience d'une IFF (figure 1), de même que ses contrôles, mesures de prévention et capacités de détection existants. En clair, une évaluation du TCFR cerne les lacunes ou les points faibles pouvant compromettre la cyberrésilience. L'IFF peut ensuite apporter des mesures correctives éclairées en accord avec ses objectifs d'affaires et sa propension à prendre des risques.




Description texte - Figure 2 – Tests d'intrusion traditionnels et méthode de l'équipe rouge comparativement au TCFR

Les tests de la cyberrésilience fondés sur le renseignement doivent respecter le processus normal d'évaluation du TCFR. Il s'agit d'un processus en continu que suivent les fournisseurs de services indépendants de piratage éthique et de collecte de renseignements sur les menaces; ils doivent appliquer ce processus à la fois à Internet, à la passerelle et au réseau local. Ce type de test aide à faire progresser les objectifs de cyberrésilience et à accroître la résilience du secteur financier et des institutions financières.

### 2.2.2. Tests d'intrusion et méthode de l'équipe rouge comparativement au TCFR

Même si les tests d'intrusion traditionnels, la méthode de l'équipe rouge et les tests de menaces fondés sur le renseignement partagent l'objectif de protéger les systèmes et les données contre les auteurs de menaces, ils diffèrent à maints égards. Comme l'indique la figure 2, le principe qui sous-tend le TCFR est que l'IFF sera soumise à une évaluation des menaces sur ses FOE en direct par des fournisseurs de services indépendants. Lors d'un TCFR, un pirate éthique, c'est-à-dire un informaticien qui effectue des tests d'intrusion, dispose de renseignements sur les menaces visant les FOE, ce qui n'est pas le cas des tests d'intrusion traditionnels et de la méthode de l'équipe rouge. Les renseignements recueillis et utilisés proviennent d'une source indépendante, c'est-à-dire un fournisseur commercial. De plus, les mesures liées à la méthode de l'équipe rouge prises par les pirates éthiques seront elles-mêmes indépendantes de l'IFF et proviendront d'un fournisseur commercial.

Le tableau 1 ci-après présente les différences notables entre les tests d'intrusion traditionnels, la méthode de l'équipe rouge et les tests de menaces fondés sur le renseignement.

### Tableau 1 : Comparaison entre les tests d'intrusion traditionnels, la méthode de l'équipe rouge et le TCFR

| | Tests d'intrusion traditionnels | Méthode de l'équipe rouge | Test de la cyberrésilience fondé sur le renseignement |
|---|---|---|---|
| Optique | Déceler les vulnérabilités connues à l'aide d'outils standards | Évaluer objectivement l'accès persistant à certains systèmes ou renseignements au moyen d'une attaque simulée | Cibler l'accès persistant à certains systèmes ou renseignements sur la base de scénarios de menace réalistes |
| Portée | L'accent est mis sur la technologie (Web, réseau, matériel, applications, etc.) | La portée va au-delà de la technologie (personnes, processus et technologie, ou PPT) | La portée va au-delà de la technologie (PPT en lien avec les FOE) |
| Approche de test | Technique connue (liste de contrôle de test des 10 principales vulnérabilités types du secteur, p. ex.) | Imitation des tactiques, techniques et procédures (TTP) des auteurs de menaces sophistiqués | Recensement de FOE cibles et imitation des TTP d'auteurs de menaces sophistiqués à partir de cybermenaces réelles |
| Objectif | Recenser autant de vulnérabilités que possible | Cerner les lacunes non seulement dans les contrôles de la technologie, mais aussi les processus et les procédures | Cerner les cybermenaces réelles et les vulnérabilités qui peuvent perturber les FOE |

Lorsqu'on parcourt le tableau 1 de gauche à droite, à mesure que le degré de sophistication du type de test augmente, le facteur distinctif du test de gauche devient une propriété inhérente de l'approche de test indiquée à droite.

Les tests d'intrusion traditionnels visent l'utilisation d'applications ou l'introduction dans un réseau pour déceler autant de vulnérabilités ou de failles de conception que possible avant qu'elles puissent être exploitées par les auteurs de menaces.

La méthode de l'équipe rouge pousse plus loin le concept de test d'intrusion en utilisant le modèle du jeu de guerre entre deux équipes. L'équipe rouge tente de s'introduire dans un réseau; elle se déplace latéralement pour éviter d'être détectée et finit par exécuter des manœuvres invasives comme la simulation de la corruption de données, la perturbation et l'exfiltration. Elle emploie habituellement des outils, des techniques et des procédures faciles à

trouver dans une source ouverte, ainsi que des procédures et des scripts perfectionnés et personnalisés pour exploiter les vulnérabilités. Il s'agit d'une façon efficace de tester et d'évaluer la capacité d'un organisme de déceler une cyberattaque et d'y réagir.

De son côté, l'équipe chargée de la cyberdéfense (p. ex., l'équipe bleue) cherche à détecter l'intrusion et à y réagir. Pour que la simulation soit réaliste, l'équipe bleue n'est pas prévenue qu'elle sera la cible d'une activité faisant appel à la méthode de l'équipe rouge.

Le TCFR résulte de l'évolution naturelle de la méthode de l'équipe rouge : il mise sur l'emploi des renseignements sur les menaces ciblées, combiné à des technologies de cyberrisque de pointe. Les auteurs de menaces sophistiqués, comme ceux parrainés par des États ou qui ont des liens avec le crime organisé, sont bien financés et utilisent des technologies de pointe. Afin d'imiter l'auteur de menaces sophistiqué, le concept de test d'intrusion fondé sur le renseignement a été élaboré par la Banque d'Angleterre avec son cadre CBEST; depuis, il a été appliqué à l'échelle internationale par d'autres autorités de contrôle (TIBER, CORIE, etc.).

Le TCFR du BSIF est l'approche du Canada en matière de test de cyberrésilience fondé sur le renseignement dans le secteur financier. Il s'inspire de ces cadres. Les synergies résultant de la combinaison de ces deux composantes se traduisent par une méthode qui permet d'imiter un auteur de menace sophistiqué.

### 2.2.3. Renseignements sur les menaces ciblées

Les renseignements sur les menaces ciblées consistent en un ensemble de scénarios de menace authentiques et réalistes qui peuvent perturber les FOE d'une IFF et servent donc de fondement à l'évaluation du TCFR. Un scénario de menace décrit les systèmes cibles de l'IFF et leurs vulnérabilités. À mesure que le paysage technologique évolue, les surfaces d'attaque des FOE peuvent également évoluer en fonction des contrôles, des processus et des procédures existants de l'IFF et de leur efficacité. Pour que les scénarios de menace soient réalistes et authentiques, les renseignements sur les menaces doivent tenir compte de la surface d'attaque évolutive d'une IFF. Ces renseignements peuvent ne pas être faciles à trouver dans une source ouverte et pourraient être fournis par un fournisseur commercial très habile qui se spécialise dans les renseignements sur les cybermenaces. Les renseignements sur les menaces ciblées doivent être :

- adaptés et ciblés en fonction du secteur financier, de l'IFF en question et de ses FOE;
- stratégiques, opérationnels et utilisables dans le cadre d'une évaluation du TCFR;
- liés aux TTP du crime organisé, des États-nations et des entités parrainées par des États (auteurs de menaces sophistiqués, p. ex.); et
- utilisés pour dresser une liste priorisée d'actifs et de systèmes vulnérables possiblement jumelée aux TTP connexes. Cette liste permet de combiner les TTP pertinentes lors de l'étape d'exécution de tests selon la méthode de l'équipe rouge (section 5.3).

### 2.2.4. Outils, techniques et procédures de pointe

Pour fournir un niveau adéquat d'assurance que les actifs et services essentiels d'une IFF sont à l'abri des auteurs de menaces très habiles, bien outillés et déterminés, le niveau et la complexité du test selon la méthode de l'équipe rouge doivent tenir compte des renseignements sur les menaces ciblées. En mettant à profit les renseignements sur les menaces ciblées, le responsable du test selon la méthode de l'équipe rouge emploie des outils, des techniques et des procédures de pointe pour simuler d'éventuelles cyberattaques par des auteurs malveillants à l'externe ou à l'interne visant les FOE de l'IFF.

### 2.2.5. Portée du TCFR et FOE

La portée d'une évaluation du TCFR est définie en fonction des FOE de l'IFF ciblée. Les FOE peuvent être décrites comme suit :

Les PPT1 requis pour la réalisation d'une activité essentielle2 et dont la perturbation pourrait avoir des conséquences sur la stabilité financière d'une société, de même que sur sa résilience, sa sûreté, sa solidité, sa clientèle ou sa conduite sur le marché. Les institutions financières dans l'ensemble du secteur appuient et fournissent ces fonctions de différentes manières à l'aide de leurs propres processus internes, lesquels reposent à leur tour sur des systèmes essentiels. Les renseignements sur les menaces spécifiques à une IFF et la méthode de l'équipe rouge visent précisément ces systèmes et les processus et personnes qui y sont associés.

### 2.2.6. Critères et fréquence d'évaluation du TCFR

Devant la multiplication des cyberincidents au pays et ailleurs dans le secteur financier, le paysage des menaces qui pèsent sur les IFF et les TTP évolue rapidement. Pour fournir une assurance continue à l'égard de la cyberrésilience, les évaluations du TCFR doivent être effectuées périodiquement. Alors que les concepts du TCFR s'appliquent en général à toutes les IFF, la portée actuelle du cadre du TCFR s'étend à l'ensemble des banques d'importance systémique (BIS) et des groupes d'assurance actifs à l'échelle internationale (GAAEI). Les recommandations du BSIF quant au moment d'effectuer un TCFR sont résumées au tableau 2 ci-dessous : Critères et fréquence d'évaluation du TCFR.

Tableau 2 : Critères et fréquence d'évaluation du TCFR

| IFF ciblées | Déclencheurs | Fréquence |
|---|---|---|
| BIS et GAAEI | Cycle de surveillance | Tous les trois ans |
| BIS et GAAEI | Risque lié aux technologies et cyberrisque pouvant menacer la stabilité financière des IFF<br><br>Importants cyberincidents menaçant la résilience opérationnelle des IFF | Déterminée par les événements |
| Autres IFF | Les IFF autres que les BIS et les GAAEI peuvent demander une évaluation du TCFR; le BSIF évaluera les demandes au cas par cas. | Au cas par cas |

Le BSIF examinera périodiquement les exigences visant l'évaluation du TCFR et sa fréquence dans le cadre de son cycle de surveillance et corrigera le tir au besoin.

## 3. Rôles et responsabilités

Le succès d'une évaluation du TCFR dépend d'une coordination soignée et de la collaboration étroite de tous les intervenants. La gouvernance, la planification, la gestion du risque et l'exécution d'une évaluation du TCFR sont confiées aux divers intervenants suivants :

- IFF et groupe de contrôle de l'IFF (GC);
- coordonnateur du groupe de contrôle (CGC);
- organisme de réglementation (BSIF);
- fournisseur de renseignements sur les menaces (FRM); et
- fournisseur de services d'équipe rouge (FSER).

## 3.1. IFF et groupe de contrôle de l'IFF (GC)

L'IFF est représentée par un cadre supérieur qui répond de l'évaluation du TCFR. L'IFF met ensuite sur pied un GC qui prend en charge la conduite de l'évaluation du TCFR. Le GC est composé de membres du personnel chevronnés participant aux interventions en réponse aux incidents de sécurité et des échelons supérieurs compétents. Le GC doit respecter les consignes suivantes :

- les membres doivent avoir des pouvoirs décisionnels pertinents;
- le nombre de membres doit être aussi limité que possible, et l'échange de renseignements, à l'intérieur comme à l'extérieur du groupe, doit être strictement régi par le besoin de savoir;
- afin de mettre en œuvre le TCFR, les membres doivent transmettre des renseignements et des connaissances essentiels au sujet des FOE, des activités commerciales, de la TI et des processus de sécurité, etc.

Il incombe au GC de procéder à l'évaluation du TCFR, ce qui comprend la gestion de projet de bout en bout, la gestion des risques, les ententes avec des fournisseurs tiers, l'établissement de la portée et les mesures correctives consécutives à l'évaluation. Le GC doit :

- désigner un coordonnateur général/responsable de l'évaluation du TCFR;
- créer un plan de gestion de projet et un document d'évaluation du risque;
- veiller à ce que l'évaluation du TCFR soit menée de façon contrôlée en recensant, en évaluant et en atténuant les risques tout au long de l'évaluation;
- cerner les points qui peuvent porter problème et les communiquer en temps opportun au BSIF (p. ex. violation du secret opérationnel [section 4.3] de l'évaluation du TCFR ou compromission présumée de l'évaluation);

- négocier, financer et gérer les ententes avec le FRM et le FSER;
- assurer la coordination et la communication avec le BSIF, le FRM et le FSER; et
- veiller à ce que les livrables soient produits conformément aux directives concernant le TCFR et transmis au BSIF en temps opportun.

La liste complète des responsabilités de l'IFF et du GC figure à l'annexe C, Matrice RACI du TCFR.

## 3.2. Coordonnateur du groupe de contrôle (CGC)

Le CGC est chargé de coordonner toutes les activités du GC mentionnées à la section 1.1, y compris l'assurance de la qualité et la gestion de projet du TCFR. Il veille à ce que tous les intervenants collaborent et s'acquittent adéquatement de leurs tâches, et il fait périodiquement le point avec les dirigeants de l'IFF et d'autres parties prenantes au besoin. Le CGC doit demander l'approbation du BSIF pour apporter toute modification à la composition du GC.

## 3.3. Organisme de réglementation

À titre d'organisme de réglementation, le BSIF exerce une supervision et fournit des consignes tout au long de l'évaluation du TCFR pour s'assurer qu'elle est effectuée en accord avec le cadre du TCFR. Il incombe au BSIF de choisir une IFF aux fins d'évaluation du TCFR sur la base des critères d'évaluation (section 2.2.6).

Les équipes du BSIF regroupent des employés compétents du Secteur de la surveillance et des spécialistes du cyberrisque qui supervisent le déroulement d'une évaluation du TCFR par l'IFF.

Plus précisément, le BSIF :

- évalue les critères de l'évaluation du TCFR et entreprend un TCFR pour une IFF ciblée si les exigences sont satisfaites;
- assure la supervision de bout en bout de l'évaluation du TCFR à toutes les étapes (amorce, collecte de renseignements sur les menaces, exécution, clôture, etc.);
- travaille avec le GC pour définir la portée du TCFR et en convenir;
- donne son avis à propos de la sélection du FRM et du FSER;

- passe en revue les constatations et le plan des mesures correctives consécutifs à l'évaluation du TCFR et rédige une lettre précisant des recommandations pour veiller à ce que les constatations fassent l'objet d'un suivi et d'une réponse en temps opportun;
- utilise les résultats de l'évaluation du TCFR pour réaliser une analyse sectorielle thématique des vulnérabilités; et
- fait un suivi des mesures correctives énoncées dans les constatations en respectant le processus standard de surveillance du BSIF jusqu'à la clôture de la lacune.

La liste complète des responsabilités du BSIF figure dans la matrice RACI (acronyme qui signifie responsable, agent comptable, consulté et informé), définie à l' annexe C, Matrice RACI du TCFR.

## 3.4. Fournisseur de renseignements sur les menaces (FRM)

Le FRM est une entreprise commerciale spécialisée dans la fourniture de renseignements et de services liés aux menaces ciblées. Le FRM a une vaste expérience de l'étude des cybermenaces et de la fourniture d'évaluations des menaces dans des domaines tels :

- les cybermenaces visant les institutions financières;
- les auteurs de menaces (État-nation, cybercriminels membres du crime organisé, etc.); et
- les outils, techniques et procédures de pointe.

Le GC négocie une entente avec le FRM pour l'exécution des tâches suivantes :

- fournir une évaluation des cybermenaces fondée sur le renseignement à l'égard de l'IFF, y compris des profils, reposant sur des preuves, d'auteurs de cybermenaces qui pourraient éventuellement cibler l'IFF;
- fournir des renseignements que d'éventuels auteurs de menaces pourraient découvrir au sujet des FOE ou de fonctions ou systèmes connexes;
- créer des scénarios de menaces fondés sur les résultats des évaluations ciblées et de la collecte de renseignements sur les menaces;
- au besoin, fournir des renseignements et tenir des consultations supplémentaires pendant l'étape d'exécution du TCFR et participer à la rédaction du rapport définitif;

- participer au bilan des activités de l'équipe rouge et des scénarios de menaces avec l'IFF, le BSIF et le FSER;
- fournir une rétroaction au sujet de la capacité de l'IFF de recueillir des renseignements sur les menaces.

La liste complète des responsabilités du FRM figure à l'annexe C, Matrice RACI du TCFR.

## 3.5. Fournisseur de services d'équipe rouge (FSER)

Le FSER est une entreprise commerciale spécialisée dans la conduite d'activités relevant de la méthode de l'équipe rouge. Il se sert des scénarios de menaces fournis par le FRM pour élaborer un plan de test de l'équipe rouge.

Le FSER doit :

- utiliser les scénarios et les modèles de menaces fournis par le FRM pour concevoir et élaborer un plan de test de l'équipe rouge (TER) ciblant les FOE et les systèmes;
- travailler de près avec le GC pour créer un plan de gestion du risque lié au TER afin de gérer le risque lié à l'application de la méthode de l'équipe rouge à des systèmes informatiques opérationnels;
- exécuter le plan de TER selon une méthode de l'équipe rouge éthique;
- faire périodiquement le point avec le GC au cours de l'évaluation selon la méthode de l'équipe rouge;
- fournir à l'IFF un rapport détaillant les résultats de l'évaluation selon la méthode de l'équipe rouge y compris les exploits, les cibles de la portée qui ont été atteintes et celles qui ne l'ont pas été;
- fournir au BSIF un rapport résumant les résultats de l'évaluation selon la méthode de l'équipe rouge, abstraction faite des renseignements confidentiels et de nature délicate propres à l'IFF;
- fournir une rétroaction au sujet de la capacité de l'IFF de déceler les incidents et d'y répondre.

La liste complète des responsabilités du FSER figure à l'annexe C, Matrice RACI du TCFR.

## 3.6. Rôle des autres organismes de réglementation

Il est entendu que les IFF mènent souvent des activités d'envergure internationale ou relevant de plus d'une administration qui sont donc également réglementées par d'autres instances (étrangères ou provinciales, p. ex.). Lorsqu'une IFF fait l'objet d'une évaluation du TCFR et que des actifs compris dans la portée sont situés sur le territoire d'une autre administration, le BSIF en informera les autorités de contrôle compétentes. Le BSIF

collaborera avec l'IFF pour veiller à ce qu'il n'y ait pas de chevauchement de portée avec les évaluations semblables effectuées à l'étranger par d'autres organismes de réglementation. Le BSIF ne divulgue pas de renseignements confidentiels de l'IFF.

# 4. Gestion du risque

La gestion du risque est essentielle à la réussite d'une évaluation du TCFR et vise à permettre au GC de demeurer en contrôle du TCFR pendant toutes les étapes.

**Étapes du TCFR**

1. Amorce
2. Collecte de renseignements sur les menaces
3. Exécution
4. Clôture

Évaluation continue du risque

## 4.1. Responsable du risque lié au TCFR

Le GC de l'IFF est chargé d'exécuter l'évaluation du risque lié au TCFR de manière contrôlée. Il doit notamment atténuer continuellement les risques recensés tout au long de l'évaluation du TCFR, comme il est indiqué ci-dessus. Plus précisément, le GC doit procéder à une évaluation initiale du risque et cerner des mesures afin d'atténuer tout risque, au besoin. La gestion du risque doit être un processus continu tout au long de l'évaluation du TCFR.

## 4.2. Considérations relatives au risque

Les principaux risques de perturbation des activités de l'IFF se manifestent à l'étape de la méthode de l'équipe rouge, soit l'étape d'exécution de l'évaluation du TCFR. L'application de la méthode de l'équipe rouge à des systèmes opérationnels ou à des FOE comporte toujours un certain niveau de risque inhérent. Le GC demeure en contrôle de l'évaluation du TCFR et peut ordonner en tout temps la cessation des activités liées à la méthode de l'équipe rouge

en cas de problème.

Le GC doit évaluer les risques touchant les aspects stratégiques et opérationnels de toutes les activités, ce qui comprend, sans s'y limiter :

- la portée du TCFR;
- les procédures de signalement aux échelons supérieurs;
- les principes de confidentialité de l'évaluation du TCFR et du besoin de savoir;
- le ciblage des FOE et des systèmes;
- le calendrier et l'échéancier du projet;
- la négociation des ententes avec des tiers fournisseurs de services;
- l'exécution des activités des tiers.

## 4.3. Secret opérationnel

Pour garantir le succès d'une évaluation du TCFR, il faut assurer le strict secret opérationnel tout au long de l'exercice. Comme on l'a vu à la section 3.2, si le secret est compromis ou si on soupçonne qu'il l'a été, le CGC doit en aviser immédiatement le BSIF. En accord avec le principe du besoin de savoir, seules certaines personnes devraient être au courant qu'une évaluation du TCFR est en préparation. Ce principe s'applique notamment aux membres de l'équipe bleue, car si ces derniers savent qu'il y aura une évaluation du TCFR, l'efficacité de l'évaluation sera grandement compromise puisque la connaissance préalable des éventuelles anomalies ou alertes ne permettra pas d'évaluer pleinement la capacité de l'équipe bleue de réagir à une cyberattaque sophistiquée.
Pour renforcer davantage la sécurité opérationnelle, un nom de code de projet est attribué à l'évaluation, et le Protocole TLP d'échange de l'information s'applique. Pour d'autres renseignements sur le protocole TLP, consultez l'annexe B - Protocole TLP.

## 4.4. Fournisseurs de services indépendants

Afin de recueillir des renseignements sur les menaces ciblées pour une portée donnée et de garantir le succès du recours à la méthode de l'équipe rouge, il est primordial de distinguer et d'isoler adéquatement les activités de collecte de renseignements sur les menaces et celles liées à la méthode de l'équipe rouge. Au nombre des

avantages immédiats du fait de confier la collecte des renseignements sur les menaces et l'exécution de la méthode de l'équipe rouge à deux fournisseurs distincts, citons l'indépendance et l'accès à des types de connaissances différents. Même si les deux fournisseurs de services doivent parfois travailler ensemble (voir l'annexe C - Matrice RACI du TCFR), leur indépendance atténue le risque d'influence découlant d'un biais conscient ou inconscient.

Du point de vue du TCFR, il est recommandé de négocier des ententes avec des fournisseurs distincts pour la collecte de renseignements sur les menaces et la méthode de l'équipe rouge. Avant de choisir des fournisseurs, l'IFF doit effectuer une vérification préalable pour s'assurer que les fournisseurs ont les compétences, l'expérience et les capacités requises pour obtenir, synthétiser et produire des renseignements sur les menaces ciblées et exécuter la méthode de l'équipe rouge. Il ne suffit pas d'effectuer une simple recherche sur le Web ou le Dark Web pour trouver des auteurs de cybermenaces et leurs outils.

Si une IFF souhaite confier la collecte de renseignements sur les menaces et la méthode de l'équipe rouge à un même fournisseur de services, il faut effectuer une évaluation au préalable pour cerner les risques et les contrôles compensatoires. Le BSIF examine l'évaluation et fournit une rétroaction. Il faut surtout établir une distinction entre les deux activités et il ne doit y avoir aucune communication ni aucun échange de renseignements entre les deux fournisseurs à moins que cela ne soit nécessaire pour assurer une plus grande collaboration, disposer de meilleurs renseignements et établir de meilleures mesures liées à la méthode de l'équipe rouge.

## 5. Processus du TCFR

Le processus du TCFR comporte quatre étapes, comme l'indique la figure 4. Ce calendrier indicatif ne doit pas être considéré comme faisant état d'une durée prédéfinie. La règle générale consiste à prévoir suffisamment de temps pour chaque étape compte tenu de la portée du TCFR. Chacune des étapes est décrite plus en détail dans les sections qui suivent. Les activités à l'origine des livrables sont également énumérées en conséquence.

**Durée des étapes**

1. Amorce (de 6 à 8 semaines)
2. Collecte de renseignements sur les menaces (de 6 à 10 semaines)

3. Exécution (de 8 à 12 semaines)
4. Clôture (de 4 à 6 semaines)

## 5.1. Étape d'amorce

L'étape d'amorce signale le début officiel du TCFR. Le BSIF mobilise formellement l'IFF, la portée de l'évaluation du TCFR est définie, et l'IFF choisit et intègre les fournisseurs de services au processus. La durée de cette étape dépend principalement du processus d'approvisionnement de l'IFF. Comme il est indiqué ci-dessus, cette étape prend environ de six à huit semaines.

**Étape d'amorce**

1. Lancement
2. Mobilisation
3. Définition de la portée
4. Approvisionnement

Le processus d'approvisionnement peut avoir lieu parallèlement à la définition de la portée du TCFR, mais la portée doit être établie avant de pouvoir achever l'étape de l'approvisionnement.

### 5.1.1. Lancement

Comme l'indique l'étape d'amorce, le lancement signale le début de l'étape d'amorce du TCFR. Après avoir choisi une IFF aux fins d'évaluation d'un TCFR, le BSIF émet une lettre officielle informant l'IFF qu'elle a été retenue pour faire l'objet du test. La lettre décrit également l'objectif, la portée et l'approche du TCFR ainsi que la production des rapports connexes.

L'extrant de cette activité est une lettre du BSIF sur le TCFR.

### 5.1.2. Mobilisation

Ayant reçu la lettre du BSIF sur le TCFR, l'IFF identifie les membres potentiels du GC et met sur pied le GC et le CGC, veillant à ce que leurs membres connaissent leurs rôles et responsabilités.

Le BSIF tient une réunion de lancement avec l'IFF; les sujets suivants y sont abordés :

- le processus du TCFR;
- les parties prenantes du TCFR ainsi que leurs rôles et responsabilités;
- les considérations contractuelles en lien avec les tiers fournisseurs de services;
- le calendrier du projet du TCFR et la gestion du risque.

Le GC prend ensuite l'initiative de créer un plan de gestion de projet qui décrit les activités d'évaluation. Afin de recenser les risques et les mesures appropriées, le GC élabore en outre un plan de gestion du risque.

Les extrants de cette activité sont :

- le plan de gestion de projet du TCFR établi par le GC;
- le document d'évaluation du risque lié au TCFR établi par le GC.

### 5.1.3. Définition de la portée

L'IFF et le BSIF travaillent en collaboration pour convenir de la portée du TCFR; ce qui mène à l'élaboration d'un document de spécification de la portée qui sera utilisé comme intrant à l'étape de l'approvisionnement.

Le BSIF fournit au GC un gabarit sur la portée du TCFR et anime un atelier avec ce dernier pour discuter des FOE de l'IFF et terminer la définition de la portée. À la suite de l'atelier, une liste de systèmes et de services clés à l'appui de chacune des FOE visées doit être établie et figurer dans le document de spécification de la portée du TCFR. Les deux parties doivent convenir de la portée avant d'aller plus loin.  Tout changement à la portée du TCFR doit faire l'objet de discussions avec le BSIF.

L'extrant de cette activité est le document de spécification établi par le GC aux fins du TCFR.

### 5.1.4. Approvisionnement

L'IFF peut entreprendre un processus d'approvisionnement parallèlement à l'établissement de la portée du TCFR. La portée d'une évaluation du TCFR doit être établie avant de choisir les fournisseurs. Comme l'indique l'étape d'amorce, la sélection et l'intégration des fournisseurs ne peuvent être achevées tant que le BSIF et le GC n'ont pas approuvé et arrêté la portée.

Il incombe à l'IFF de sélectionner le FRM et le FSER, de négocier des ententes avec eux et de les rémunérer. Le BSIF peut donner son avis sur la sélection des fournisseurs, mais l'IFF est responsable de tous les aspects du processus d'approvisionnement.

## 5.2. Étape de collecte de renseignements sur les menaces

Cette étape vise à mettre au point des scénarios de cybermenaces réalistes (c.-à-d. un profil de cybermenaces) pour l'IFF en tenant compte de la portée établie à l'étape d'amorce. Cette étape est déterminante puisqu'elle jette les bases de l'étape d'exécution, celle durant laquelle se déroulent les activités de la méthode de l'équipe rouge. Pour dresser un profil de cybermenaces réaliste, le GC fournit d'abord une orientation au FRM. Le FRM recueille des renseignements sur les menaces, puis crée le rapport de renseignements sur les menaces. En outre, il doit évaluer la capacité de l'IFF en lien avec les renseignements sur les menaces et en communiquer le résultat.

**Étape de collecte de renseignements sur les menaces**

1. Orientation
2. Renseignements
3. Examen
4. Évaluation

### 5.2.1. Orientation

Le GC communiquera le document sur la portée au FRM et au FSER. Il décidera également s'il faut fournir au FRM les différentes informations au sujet de l'IFF comme la documentation opérationnelle et technique sur les systèmes,

les résultats d'évaluations antérieures des menaces et l'information sur les récents événements pertinents. Le FRM pourra ensuite tenir compte de ces informations pour établir un plan relatif aux renseignements sur les menaces axé sur les FOE de l'IFF.

L'extrant de cette activité est le plan relatif aux renseignements sur les menaces établi par le FRM.

### 5.2.2. Renseignements

À partir du plan relatif aux renseignements sur les menaces, le FRM recueille, analyse, examine et consolide des renseignements pertinents sur les menaces pour une période donnée. Ces renseignements, qui proviennent de différentes sources, y compris les renseignements sur les menaces dont dispose l'IFF elle-même, sont consolidés de façon structurée pour obtenir le profil formel des cybermenaces de l'IFF aux fins de l'évaluation du TCFR. Comme on l'a vu à la section 2.2.3, l'information sur les menaces peut comprendre des descriptions très générales des vulnérabilités technologiques et cybernétiques, les auteurs de menaces, leurs TTP, les vecteurs des menaces et des indicateurs de compromission en lien avec les FOE.

Une fois ces activités terminées, le FRM élabore des scénarios de menaces qui décrivent les comportements des auteurs de menaces et leurs répercussions sur les fonctions ciblées. Ces scénarios sont ensuite mis en correspondance avec une ou plusieurs FOE. On obtient ainsi essentiellement le profil des cybermenaces qui pèsent sur les FOE de l'IFF. Le FRM utilise ensuite l'information liée à ce profil pour produire le rapport de renseignements sur les menaces. La description contenue dans le rapport correspond essentiellement au profil de cybermenaces des scénarios et comprend notamment :

- l'objectif et la cible de l'attaque;
- des renseignements au sujet de l'auteur des menaces et de ses intentions;
- les TTP.

Le CGC transmet le rapport de renseignements sur les menaces aux intervenants pertinents (FSER, BSIF, etc.) à titre informatif. Le rapport étant prêt, le FSER peut commencer à rédiger un plan initial du TER.

Les extrants de cette activité sont :

- le rapport initial de renseignements sur les menaces, dressé par le FRM;
- le plan initial du test de l'équipe rouge, dressé par le FSER.

### 5.2.3. Examen

Une fois produit, le rapport de renseignements sur les menaces est transmis aux intervenants pertinents (IFF, FSER, BSIF, etc.) aux fins d'examen et de commentaires. Le BSIF organise un atelier avec l'IFF, le FRM et le FSER pour s'assurer que le profil de risque est réaliste et qu'il reflète les FOE comprises dans la portée. Après cet atelier, le FRM consolide les mesures en découlant et produit la version définitive du rapport de renseignements sur les menaces. Le rapport est ensuite examiné par le BSIF puis approuvé et accepté par le GC.

Le FSER pourrait devoir réviser le plan initial du TER dans la foulée de l'atelier et en tenant compte des risques recensés. Enfin, le GC examine le plan de projet du TCFR et l'évaluation du risque à la lumière de l'atelier. Le CGC veille à ce que les principaux intervenants soient au fait de toute modification liée aux risques et aux mesures figurant dans l'évaluation du TCFR.

Les extrants de cette activité sont :

- la version définitive du rapport de renseignements sur les menaces dressé par le FRM;
- le plan de test de l'équipe rouge révisé par le FSER;
- le plan de projet du TCFR révisé par le GC;
- l'évaluation du risque révisée par le GC.

### 5.2.4. Évaluation

L'évaluation est la dernière activité de l'étape de collecte de renseignements sur les menaces. C'est ici que le FRM donne son opinion au sujet des capacités de l'IFF en matière de renseignements sur les menaces.

## 5.3. Exécution

Une fois le profil des cybermenaces de l'IFF à l'étape de collecte de renseignements sur les menaces achevé, le FSER prend les commandes. Au cours de l'étape d'exécution, les spécialistes du FSER assument le rôle d'auteurs de menaces et mènent les activités invasives proprement dites (selon la méthode de l'équipe rouge) qui ciblent les

actifs de l'IFF associés aux FOE visées par la portée. Avant le début de cette étape, le BSIF peut informer le Centre canadien pour la cybersécurité de la tenue de ces activités.

Afin d'obtenir une évaluation exhaustive, il faut prévoir suffisamment de temps pour l'exécution du plan de TER. Bien que la durée de l'étape d'exécution dépende de nombreux facteurs comme la portée, les ressources, etc., l'expérience à ce jour montre que l'étape d'exécution d'une évaluation du TCFR est celle à laquelle on consacre le plus de temps (se reporter à la rubrique durée des étapes). Il importe de répéter qu'il est essentiel de préserver le secret opérationnel (décrit à la section 4.3) pendant toute l'étape d'exécution pour obtenir une vue d'ensemble crédible de la cyberrésilience de l'IFF. Les résultats du TER sont documentés dans les rapports appropriés. Dans le cadre de l'étape d'exécution, le FSER doit donner son avis au sujet de la capacité de l'IFF de déceler les incidents et d'y réagir.

**Étape d'exécution**

1. Planification
2. Méthode de l'équipe rouge
3. Examen
4. Évaluation

### 5.3.1. Planification

Puisque le FSER est déjà au courant de la portée du TCFR et qu'il a accès au rapport de renseignements sur les menaces, il peut achever le plan de TER initial créé à l'étape de collecte de renseignements sur les menaces. À cette fin, pour chaque scénario abordé dans le rapport de renseignements sur les menaces, le FSER élabore des scénarios pour le test de l'équipe rouge, comme prévu dans le plan de TER. Il doit détailler les étapes à suivre, ainsi que les outils, techniques et procédures de pointe utilisés. La version définitive du plan de TER doit décrire comment un scénario prend en compte :

- les scénarios de menaces décrits par le FRM dans le rapport de renseignements sur les menaces;
- les FOE décrites dans le document de spécification de la portée du TCFR.

Toute activité relevant de la méthode de l'équipe rouge comporte un niveau de risque pour les FOE. Il faut réduire au strict minimum les risques pour l'IFF comme la détérioration ou l'interruption des services ou la divulgation de renseignements de nature sensible. De concert avec le FSER, le GC doit donc inclure un plan approprié de gestion de ces risques. Le GC doit examiner et approuver le plan du FSER et l'évaluation du risque avant d'aller plus loin.

Les extrants de cette activité sont :

- la version définitive du plan de test de l'équipe rouge, dressé par le FSER;
- le plan de gestion du risque lié au TER, dressé par le GC et le FSER.

### 5.3.2. Méthode de l'équipe rouge

Une fois l'étape de planification achevée, le FSER effectue un TCFR sur les actifs et les services ciblés (c.-à-d. les FOE), déterminés à l'étape de la définition de la portée (section 5.1.3). À mesure que l'équipe rouge avance dans le plan établi à son intention, elle doit tenter d'atteindre les objectifs d'auteurs de menaces fixés à l'étape de collecte de renseignements sur les menaces (section 5.2).

À l'instar du FRM, le FSER est soumis à des contraintes de temps et de ressources, de même qu'à des balises morales, éthiques et juridiques. Il se pourrait donc que le FSER et l'IFF discutent de la possibilité de modifier la séquence des étapes, voire d'en sauter, si l'évaluation progresse lentement. Toute activité en ce sens devra être approuvée par le BSIF. En pareil cas, le FSER obtient une certaine aide pour passer à l'étape suivante de l'attaque afin de tester des vulnérabilités qu'il n'aurait pas le temps de mettre à l'essai autrement.

Les résultats des activités menées par l'équipe rouge fournissent des renseignements sur les vulnérabilités critiques, et peuvent aussi indiquer des faiblesses ou des lacunes sur le plan des contrôles, des processus et des procédures. Ils doivent inclure des recommandations de la part du FSER. Pour que les résultats soient communiqués selon le principe du besoin de savoir, le FSER produit deux versions du rapport sur le TER, l'une pour l'IFF et l'autre pour le BSIF. Même si les deux rapports contiennent une description des résultats des scénarios de menaces et des tests pertinents, celui destiné au BSIF ne doit renfermer aucun renseignement confidentiel ou de nature délicate comme des données à caractère personnel et des spécifications techniques comme des adresses IP, des noms de système, des précisions sur la configuration, etc.

Les extrants de cette activité sont :

- le rapport initial sur le test de l'équipe rouge, dressé par le FSER à l'intention de l'IFF;
- le rapport initial sur le test de l'équipe rouge, dressé par le FSER à l'intention du BSIF.

### 5.3.3. Examen

Le GC, le BSIF, le FSER et le FRM tiennent un atelier pour examiner les résultats du test de l'équipe rouge détaillés dans le rapport provisoire sur le test de l'équipe rouge. L'atelier est organisé par le BSIF pour discuter :

- des conditions de l'exécution du TER et des vulnérabilités cernées (sous la direction du FSER);
- des facteurs d'atténuation et des mesures correctives proposées (sous la direction du GC).

Le FSER mettra la dernière main aux rapports sur le TER sur la base des discussions tenues lors de l'atelier.

À la suite de l'atelier, le GC doit amorcer l'élaboration d'un plan provisoire de mesures correctives en fonction des vulnérabilités et des recommandations découlant du TER.

Les extrants de cette activité sont :

- le rapport définitif du FSER sur le TER à l'intention de l'IFF;
- le rapport définitif du FSER sur le TER à l'intention du BSIF;
- le plan initial de mesures correctives du GC.

### 5.3.4. Évaluation

Il s'agit de la dernière activité de l'étape d'exécution. C'est d'ailleurs au cours de cette activité que le FSER donne son avis au sujet de la capacité de l'IFF de déceler les incidents et d'y réagir.

## 5.4. Clôture

Une fois l'étape d'exécution terminée, l'évaluation du TCFR passe à l'étape de clôture. À cette étape, l'IFF met la dernière main au plan de mesures correctives et le BSIF émet une lettre de surveillance qui renferme un sommaire des constatations et des recommandations à l'IFF. Le BSIF s'attend à ce que chaque constatation soit assortie d'une réponse formelle et de plans de mesures correctives qui feront l'objet d'un suivi dans le cadre du processus normal

de surveillance.

**Étape de clôture**

1. Mesures correctives
2. Surveillance

### 5.4.1. Mesures correctives

Étape essentielle aux fins d'apprentissage, tous les intervenants assistent à un compte rendu des activités de l'équipe rouge comprenant un examen de l'évaluation des cybermenaces effectuée par le FRM et le FSER.

Utilisant une approche fondée sur le risque, le GC achève le plan initial de mesures correctives élaboré à l'étape d'exécution du TCFR.

À l'instar de tous les autres travaux de surveillance, le BSIF analyse les faits (c.-à-d. le rapport sur le TER) et effectue ses propres observations tout au long de l'évaluation du TCFR. À partir de cette analyse et de l'examen, le BSIF peaufine ses constatations et recommandations puis les présente à l'IFF lors d'un entretien récapitulatif. Le BSIF transmet ensuite à l'IFF une lettre de surveillance qui résume ses constatations et recommandations. L'IFF doit fournir des plans d'action détaillés relativement aux constatations présentées dans la lettre du BSIF. Le BSIF utilise les résultats de l'évaluation du TCFR pour réaliser une analyse sectorielle thématique des vulnérabilités.

Dans sa lettre, le BSIF peut inclure une « attestation TCFR » selon laquelle l'IFF a fait l'objet d'une évaluation du TCFR conforme aux exigences du cadre du TCFR. Le BSIF se réserve le droit de refuser d'accorder cette attestation si l'IFF ne respecte pas entièrement les exigences du cadre.

L'extrant de cette activité est une lettre de surveillance du BSIF.

### 5.4.2. Surveillance

Après avoir envoyé sa lettre de surveillance, le BSIF fait un suivi des activités correctives de l'IFF jusqu'à ce que toutes les constatations soient closes. Les constatations et recommandations formulées dans la lettre de surveillance sont traitées comme celles découlant d'un examen de surveillance et nécessiteront des preuves à

l'appui de leur clôture.

## 6. Mentions légales

Les renseignements et les concepts présentés ici le sont à titre informatif seulement. Le cadre du TCFR ne constitue pas une source de conseils juridiques ou professionnels, et l'information ne doit pas être utilisée ou traitée comme se substituant à des conseils précis en lien avec des circonstances particulières. Le BSIF décline toute responsabilité en cas d'erreur, d'omission ou de mauvaise interprétation des énoncés formulés dans le présent document, ou de perte résultant de l'utilisation des renseignements et des concepts qui y sont présentés.

## 7. Annexe A – Glossaire

**CBEST**

Cadre de cyberrésilience de l'Autorité de régulation prudentielle (PRA) de la Banque d'Angleterre.

**CGC**

Coordonnateur du groupe de contrôle - Le CGC est chargé de la coordination générale des activités pour l'IFF.

**CORIE**

Cyber Operational Resilience Intelligence-led Exercises (exercices de cyberrésilience opérationnelle fondés sur le renseignement).

**FOE**

Les fonctions opérationnelles essentielles (FOE) déterminent la portée de l'évaluation du TCFR. Les FOE représentent les personnes, les processus et les technologies requises pour la réalisation d'une activité essentielle[2] et dont la perturbation pourrait avoir des conséquences sur la stabilité financière d'une société, de même que sur sa résilience, sa sûreté, sa solidité, sa clientèle ou sa conduite sur le marché. Les institutions financières dans l'ensemble du secteur appuient et fournissent ces fonctions de différentes manières à l'aide de leurs propres processus internes, lesquels reposent à leur tour sur des systèmes essentiels. Les renseignements sur les menaces spécifiques à une IFF et la méthode de l'équipe rouge visent précisément ces systèmes et les processus et personnes qui y sont associés.

**FRM**

Le fournisseur de renseignements sur les menaces (FRM) est responsable de l'étape de collecte de renseignements sur les menaces.

**FSER**

Le fournisseur de services d'équipe rouge (FSER) est responsable de la conduite d'activités relevant de la méthode de l'équipe rouge qui sont exécutées au cours de l'étape d'exécution.

**GC**

Groupe de contrôle - Le GC prend en charge la gestion de l'évaluation du TCFR.

**IFF**

Institutions financières fédérales.

**TER**

Activités liées au test de l'équipe rouge menées par le FSER.

**Test de la cyberrésilience fondé sur le renseignement (TCFR)**

Ce test mesure la résilience d'un organisme pour déceler une cyberattaque, y réagir et y résister. Il se distingue d'un exercice d'équipe rouge et d'un test d'intrusion puisque des tiers indépendants fournissent des scénarios de menace réalistes contre les FOE à d'autres tiers indépendants qui s'en servent pour imiter les auteurs de menaces sophistiqués; la cyberattaque est menée à l'aide d'outils, de techniques et de procédures spécialement conçus.

**TIBER**

Test fondé sur le renseignement selon la méthode de l'équipe rouge éthique.

# 8. Annexe B – Protocole TLP

Le secret opérationnel et le respect du principe du besoin de savoir sont essentiels au succès du TCFR.

L'information doit être protégée et partagée en fonction du besoin de savoir. Voici des consignes sur le traitement de l'information.

## Objet et contexte

Le BSIF convient qu'une communication efficace, cohérente et coordonnée fait partie intégrante du succès du projet **NOM** (le « projet »).

Le présent document décrit une approche globale en vue de communiquer l'information de manière efficace tout au long du cycle de vie du projet.

## Traitement de l'information

L'exactitude, la confidentialité et l'exhaustivité de l'information constituent d'importants actifs du *projet* **NOM** et des facteurs déterminants de sa réussite. Il importe de préserver tout autant la sécurité que l'intégrité de l'information de nature délicate créée dans le cadre de ce projet.

Pour assurer le traitement cohérent de l'information liée au projet, tous les documents doivent être étiquetés de façon appropriée.

## Protocole TLP

Ce protocole TLP[3] a été élaboré pour faciliter l'échange d'information. Il s'agit d'un système de classification conçu pour veiller à ce que l'échange d'information de nature délicate soit effectué avec l'auditoire approprié. Un code de trois (3) couleurs est utilisé pour indiquer les paramètres que les destinataires doivent respecter quant à l'échange d'information.

Le protocole TLP du *projet***NOM** ne comporte que trois couleurs; aucun autre type de classification non mentionné dans le présent document n'est considéré comme valide. Tous les documents liés au projet, y compris les courriels, doivent comporter l'étiquette TLP appropriée. Si un destinataire estime que l'information doit être diffusée plus largement que prévu par l'étiquette TLP initiale, il doit obtenir l'autorisation explicite de la source originale.

Utilisation générale : pour étiqueter un document, écrire en lettres majuscules de la couleur appropriée, en caractères gras.

À noter toutefois que ces étiquettes ne remplacent pas les déclarations de confidentialité ou les ententes à cet effet.

TLP du projet nom

| Couleur | Modalités de diffusion | Exemple |
|---|---|---|
| TLP : **ROUGE**<br><br>Ne pas communiquer; réservé aux destinataires | Les destinataires **ne peuvent pas** échanger de l'information dont le code TLP est **ROUGE** avec quiconque en dehors des participants à l'échange, à la réunion ou à la conversation au cours duquel ou de laquelle les renseignements ont été communiqués au départ. | L'information classifiée **ROUGE** selon le TLP est réservée aux personnes présentes à la réunion et aux destinataires d'un courriel provenant de la source. |
| TLP : **JAUNE + STRICT**<br><br>Communication limitée aux membres de l'entité participant au *projet* ***NOM***. | Les destinataires peuvent seulement échanger de l'information dont le code TLP est **JAUNE +STRICT** avec les membres de leur propre l'entité qui participent directement au *projet* ***NOM***. L'information **ne doit pas** être échangée avec les fournisseurs (FRM et FSER). | L'information classifiée **JAUNE + STRICT** selon le TLP qui est communiquée lors d'une réunion peut seulement être transmise aux membres de l'entité. |
| TLP : **JAUNE**<br><br>Communication limitée aux participants au *projet* ***NOM*** qui proviennent de nos entités respectives. | Les destinataires ne peuvent échanger de l'information dont le code TLP est **JAUNE** qu'avec les membres de leur propre entité qui participent directement au *projet* ***NOM*** et avec les fournisseurs (FRM et FSER) qui ont **« besoin de savoir »**. | L'information classifiée **JAUNE** selon le TLP qui est communiquée lors d'une réunion peut être transmise à des personnes autres que les participants sous réserve d'un besoin de savoir légitime. |
| TLP : **VERT**<br><br>Communication limitée aux employés de nos entités respectives. | Les sources peuvent utiliser le code TLP : **VERT** si l'information est utile pour sensibiliser l'ensemble des personnes et des entités participantes; elles peuvent aussi communiquer l'information à des pairs de l'ensemble d'un groupe élargi ou du secteur. Les destinataires peuvent échanger de l'information dont le code TLP est **VERT** avec des pairs ou des collègues de leur entité, mais non par l'entremise de canaux accessibles au public. | L'information classifiée **VERT** selon le TLP peut être communiquée à grande échelle au sein d'un groupe donné (c.-à-d. l'IFF, le BSIF et les tiers qui sont parties à des marchés liés au *projet* ***NOM***), mais non à l'extérieur de celui-ci. |

## 9. Annexe C – Matrice RACI du TCFR

La liste complète des rôles et responsabilités des différents intervenants en ce qui concerne le TCFR figure ci-après dans la matrice RACI [acronyme qui signifie responsable (R), agent comptable (A), consulté (C) et informé (I)].

## Matrice RACI du TCFR pour l'étape d'amorce, par intervenant

| Sous-étape | Description | Cadre responsable au sein de l'IFF | GC | BSIF | FRM | FSER |
|---|---|---|---|---|---|---|
| Lancement | Évaluation du besoin d'effectuer un TCFR | - | - | R/A | - | - |
| | Envoi d'une lettre à l'IFF | I | - | R/A | - | - |
| Mobilisation | Constitution et établissement du groupe de contrôle (GC) du TCFR | A/R | - | C | - | - |
| | Désignation et affectation du coordonnateur du GC | A/R | R | C | - | - |
| | Atelier de mobilisation et réunion de lancement | A | C | R | - | - |
| | Création du plan de gestion de projet du TCFR | A | R | I | - | - |
| | Création du document d'évaluation du risque du TCFR | A | R | I | - | - |
| Définition de la portée | Création du document de spécification de la portée | A | R | C | - | - |
| | Coordination de l'atelier sur l'établissement de la portée | A | C | R | - | - |
| | Acceptation du document sur la portée | A | R | R | - | - |
| Approvisionnement | Amorce du processus d'approvisionnement | R/A | C | I | - | - |
| | Définition des critères de sélection des fournisseurs | R/A | C | C | - | - |
| | Sélection des fournisseurs pour le FRM et le FSER | A | R | C | I | I |
| | Intégration des fournisseurs (FRM et FSER) et confirmation de la préparation en vue d'amorcer l'étape de collecte de renseignements sur les menaces | A | R | C | C | C |

## Matrice RACI du TCFR pour l'étape de collecte de renseignements sur les menaces, par intervenant

| Sous-étape | Description | Cadre responsable au sein de l'IFF | GC | BSIF | FRM | FSER |
|---|---|---|---|---|---|---|
| Orientation | Communication du document sur la portée au FRM et au FSER | A | R | I | I | I |
| | Communication de renseignements pertinents (aperçu opérationnel et technique des systèmes, évaluation actuelle des menaces pour l'IFF, exemples d'attaques ou d'incidents récents, etc.) au FRM | A | R | I | C | - |
| | Examen des FOE, des systèmes connexes et de l'évaluation des menaces | A | C | I | R | - |
| | Production du plan relatif aux renseignements sur les menaces | A | C | C | R | - |
| Renseignements | Exécution de l'évaluation des renseignements sur les menaces | A | C | I | R | I |
| | Création du rapport de renseignements sur les menaces | A | C | C | R | I |
| | Amorce de l'élaboration du plan initial du test de l'équipe rouge (TER) | A | C | C | C | R |
| Examen | Atelier d'examen | A | C | R | C | C |
| | Acceptation des rapports de renseignements sur les menaces | A | R | C | I | I |
| | Supervision réglementaire des rapports de renseignements sur les menaces | A | I | R | I | I |
| Évaluation | Formulation d'une opinion au sujet de la capacité de l'IFF en matière de renseignements sur les menaces | A | C | I | R | - |

## Matrice RACI du TCFR pour l'étape d'exécution , par intervenant

| Sous-étape | Description | Cadre responsable au sein de l'IFF | GC | BSIF | FRM | FSER |
|---|---|---|---|---|---|---|
| Planification | Achèvement du plan de test de l'équipe rouge (TER) | A | C | C | I | R |
| | Création du document d'évaluation du risque du TER | A | R | C | I | R |
| | Acceptation du plan de TER et de l'évaluation du risque du TER | A/R | R | I | I | I |
| Méthode de l'équipe rouge | Exécution du TER | A | C | C | - | R |
| | Création d'un rapport sur le TER à l'intention de l'IFF (rapport détaillé et technique à l'IFF) | A | C | C | - | R |
| | Création d'un rapport sur le TER à l'intention du BSIF (ne doit pas contenir de renseignements confidentiels) | A | C | C | - | R |
| Examen | Atelier consacré à l'examen | A | C | R | C | C |
| | Acceptation du rapport sur le TER | A | R | C | I | I |
| | Supervision réglementaire du rapport sur le TER | A | I | R | I | I |
| Évaluation | Formulation d'une opinion au sujet de la capacité de l'IFF de déceler les incidents et d'y réagir | A | C | I | - | R |

Matrice RACI du TCFR pour l'étape de clôture, par intervenant

| Sous-étape | Description | Cadre responsable au sein de l'IFF | GC | BSIF | FRM | FSER |
|---|---|---|---|---|---|---|
| Mesures correctives | Compte rendu des activités liées au TER et des scénarios de cybermenaces | A | R | I | R | R |
| | Création d'un plan de mesures correctives fondé sur le risque | A | R | I | - | - |
| | Achèvement des constatations et des recommandations | I | I | R/A | - | - |
| | Tenue de l'entretien récapitulatif | C | C | R/A | - | - |
| | Envoi de la lettre de surveillance | I | I | R/A | - | - |
| Surveillance | Suivi des problèmes jusqu'à leur résolution | I | I | R/A | - | - |

# 10. Annexe D – Outils supplémentaires

## 10.1. Gabarits

Les gabarits du TCFR définissent les attentes en lien avec les tâches associées à différentes étapes de l'évaluation du TCFR. Ils fournissent les rubriques, les sujets et les sections nécessaires pour saisir et présenter l'information de manière structurée. Une liste de gabarits du TCFR est présentée ci-dessous.

- Spécification de la portée du TCFR
- Spécification du rapport de renseignements sur les menaces du TCFR
- Spécifications du rapport sur le test de l'équipe rouge du TCFR

1 Peut comprendre les actifs et les services de tiers comme le nuage public.

2 Définitions clés liées à la résilience opérationnelle

3 D'après le modèle TLP établi par le Forum of Incident Response and Security Teams (FIRST) (en anglais seulement)