Journal officiel
de l'Union européenne

FR
Série L

2025/1190

18.6.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/1190 DE LA COMMISSION

du 13 février 2025

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les critères utilisés pour identifier les entités financières tenues d'effectuer des tests d'intrusion fondés sur la menace, les exigences et les normes régissant le recours à des testeurs internes, les exigences relatives au périmètre et à la méthodologie des tests ainsi qu'à l'approche à suivre pour chaque phase des stades de test, de résultats, de clôture et de correction et le type de coopération en matière de surveillance et les autres types de coopération pertinents qui sont nécessaires pour l'exécution des tests d'intrusion fondés sur la menace et pour la facilitation de la reconnaissance mutuelle

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 ([1]), et plus particulièrement son article 26, paragraphe 11, quatrième alinéa,

considérant ce qui suit:

(1) Le présent règlement a été élaboré conformément au cadre TIBER-EU et reproduit la méthodologie, le processus et la structure des tests d'intrusion fondés sur la menace (TIFM) décrits dans TIBER-EU. Les entités financières soumises à des TIFM peuvent se référer au cadre TIBER-EU, ou à l'une de ses transpositions nationales, et l'appliquer, dans la mesure où ce cadre ou cette transposition est conforme aux exigences énoncées aux articles 26 et 27 du règlement (UE) 2022/2554 et dans le présent règlement. La désignation d'une autorité publique unique au sein du secteur financier chargée des questions liées aux tests d'intrusion fondés sur la menace au niveau national conformément à l'article 26, paragraphe 9, du règlement (UE) 2022/2554 devrait être sans préjudice des compétences confiées à des autorités au niveau de l'Union en ce qui concerne la surveillance de certaines entités financières conformément à l'article 46 dudit règlement, par exemple, à la Banque centrale européenne pour les établissements de crédit classés comme importants, qui doivent être considérées comme compétentes pour les questions liées aux tests d'intrusion fondés sur la menace. Lorsque seule une partie des tâches liées aux tests d'intrusion fondés sur la menace est déléguée à une autre autorité nationale du secteur financier conformément à l'article 26, paragraphe 10, du règlement (UE) 2022/2554, l'autorité compétente de l'entité financière visée à l'article 46 dudit règlement devrait rester l'autorité chargée des tâches liées aux TIFM qui n'ont pas été déléguées.

(2) Compte tenu de la complexité des tests d'intrusion fondés sur la menace et des risques y afférents, leur utilisation devrait être limitée aux entités financières pour lesquelles elle est justifiée. Par conséquent, les autorités responsables des questions relatives aux TIFM (les «autorités TIFM», au niveau de l'Union ou au niveau national) devraient exclure du champ d'application des TIFM les entités financières qui exercent leurs activités dans des sous-secteurs essentiels de services financiers pour lesquels un TIFM n'est pas justifié. Cela signifie que des établissements de crédit, des établissements de paiement et de monnaie électronique, des dépositaires centraux de titres, des contreparties centrales, des plates-formes de négociation et des entreprises d'assurance et de réassurance, même s'ils remplissent les critères quantitatifs, pourraient être dispensés de l'exigence de TIFM à la lumière d'une évaluation globale de leur profil de risque lié aux TIC et de la maturité de leurs TIC, de leur incidence sur le secteur financier et des préoccupations relatives à la stabilité financière.

(3) Les autorités TIFM devraient évaluer, à la lumière d'une évaluation globale du profil de risque lié aux TIC et de la maturité des TIC, de l'incidence sur le secteur financier et des préoccupations relatives à la stabilité financière, s'il convient qu'un type d'entité financière autre que les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique, les contreparties centrales, les dépositaires centraux de titres, les plates-formes de négociation et les entreprises d'assurance et de réassurance soit soumis à des TIFM. L'évaluation visant à déterminer si ces entités financières satisfont à ces critères qualitatifs devrait viser à identifier, au moyen d'indicateurs intersectoriels et objectifs, les entités financières pour lesquelles un TIFM est approprié. Dans le même temps,

([1]) JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

l'évaluation visant à déterminer si une entité financière satisfait à ces critères qualitatifs devrait faire en sorte que les entités soumises à des tests d'intrusion fondés sur la menace soient uniquement celles pour lesquelles un tel test est justifié. La question de savoir si une entité financière satisfait à ces critères qualitatifs devrait également être évaluée à la lumière de l'évolution des nouveaux marchés et de l'importance croissante que prendront à l'avenir de nouveaux acteurs du marché pour le secteur financier, dont les prestataires de services sur crypto-actifs agréés conformément à l'article 59 du règlement (UE) 2023/1114 du Parlement européen et du Conseil ([2]).

(4) Des entités financières peuvent avoir le même prestataire de services TIC intra-groupe ou appartenir au même groupe et dépendre de l'utilisation de systèmes de TIC partagés. Dans ce cas, pour évaluer si une entité financière doit être soumise à des tests d'intrusion fondés sur la menace et si ces tests doivent être conduits au niveau de l'entité ou au niveau du groupe (au moyen d'un TIFM commun), il est important que les autorités TIFM tiennent compte de la structure et du caractère systémique ou de l'importance pour le secteur financier de cette entité financière au niveau national ou au niveau de l'Union.

(5) Pour être conforme au cadre TIBER-EU, il est nécessaire que la méthodologie des tests prévoie la participation des principaux participants suivants: l'entité financière, avec une équipe chargée du contrôle (correspondant à l'«équipe chargée du contrôle» de TIBER-EU) et une équipe bleue (correspondant à l'«équipe bleue» de TIBER-EU), et l'autorité TIFM, sous la forme d'une équipe de cybersécurité TIFM (correspondant aux «cyberéquipes TIBER» de TIBER-EU), un fournisseur de renseignements sur les menaces et des testeurs (les testeurs correspondant au «fournisseur de l'équipe rouge» de TIBER-EU).

(6) Afin de faire en sorte que les TIFM bénéficient de l'expérience acquise dans le cadre de la mise en œuvre de TIBER-EU et de réduire les risques associés à l'exécution des TIFM, il convient de veiller à ce que les responsabilités des équipes de cybersécurité TIFM mises en place au niveau des autorités TIFM correspondent le plus étroitement possible à celles des équipes de cybersécurité de TIBER-EU. Par conséquent, les équipes de cybersécurité TIFM devraient comprendre des gestionnaires de test chargés de superviser les TIFM ainsi que de planifier et de coordonner les différents tests. Les équipes de cybersécurité TIFM devraient servir de point de contact unique pour la communication concernant les tests avec les parties prenantes internes et externes, pour la collecte et le traitement des retours d'information et des enseignements tirés des tests conduits précédemment, et pour l'assistance aux entités financières faisant l'objet de tests d'intrusion fondés sur la menace.

(7) Conformément à la méthodologie du cadre TIBER-EU, les gestionnaires de test devraient disposer des compétences et des capacités nécessaires pour fournir des conseils et remettre en question les propositions des testeurs. L'expérience acquise avec le cadre TIBER-EU a démontré qu'il est utile qu'une équipe d'au moins deux gestionnaires soit affectée à chaque test. Afin de tenir compte du fait que le TIFM est utilisé pour encourager l'expérience d'apprentissage, en vue de préserver la confidentialité des tests, et à moins qu'elles n'aient des problèmes de ressources ou d'expertise, les autorités TIFM sont vivement encouragées à considérer que, pendant la durée d'un TIFM, les gestionnaires de test ne doivent pas exercer d'activités de surveillance sur l'entité financière faisant l'objet de ce TIFM.

(8) Il importe, dans un souci de cohérence avec le cadre TIBER-EU, que l'autorité TIFM suive de près le processus de test à chacun de ses stades. Compte tenu de la nature des tests et des risques qui y sont associés, il est fondamental que l'autorité TIFM intervienne à chaque phase spécifique des tests. L'autorité TIFM devrait ainsi être consultée et valider les évaluations ou décisions des entités financières susceptibles, d'une part, d'influer sur l'efficacité des tests et, d'autre part, d'avoir une incidence sur les risques associés à ceux-ci. Les étapes fondamentales pour lesquelles une intervention spécifique de l'autorité TIFM est nécessaire comprennent la validation de certains documents essentiels relatifs aux tests, et la sélection de fournisseurs de renseignements sur les menaces et de testeurs et de mesures de gestion des risques. L'intervention des autorités TIFM, en particulier pour les validations, ne devrait pas entraîner de charge excessive pour ces autorités et devrait donc se limiter aux documents et décisions qui ont une incidence directe sur la conduite des TIFM. Grâce à leur participation active à chaque phase des tests, les autorités TIFM peuvent effectivement évaluer le respect, par les entités financières, des exigences applicables, ce qui devrait permettre à ces autorités de délivrer des attestations conformément à l'article 26, paragraphe 7, du règlement (UE) 2022/2554.

([2]) Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (JO L 150 du 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) La confidentialité du TIFM est de la plus haute importance pour garantir que les conditions du test soient réalistes. Pour cette raison, les tests devraient être effectués en secret, et des précautions devraient être prises pour en préserver la confidentialité, notamment grâce au choix de noms de code conçus pour empêcher l'identification des TIFM par des tiers. Si les membres du personnel chargés de la sécurité de l'équipe financière devaient apprendre qu'un TIFM est prévu ou en cours, il est probable qu'ils seraient plus attentifs et plus vigilants que dans des conditions de travail normales, ce qui altérerait les résultats des tests. Les membres du personnel de l'entité financière qui ne font pas partie de l'équipe chargée du contrôle ne devraient donc être informés qu'un TIFM est prévu ou en cours que s'il existe des raisons valables de le faire, et moyennant l'accord préalable des gestionnaires de test, notamment pour garantir la confidentialité du test dans l'hypothèse où un membre de l'équipe bleue l'aurait détecté.

(10) Comme le montre l'expérience acquise avec le cadre TIBER-EU s'agissant de l'«équipe chargée du contrôle», pour que les TIFM soient conduits en toute sécurité, il est indispensable de bien sélectionner le chef de l'équipe chargée du contrôle. Celui-ci devrait disposer, au sein de l'entité financière, du mandat nécessaire pour piloter tous les aspects des tests, sans en compromettre la confidentialité. Pour la même raison, les membres de l'équipe chargée du contrôle devraient avoir une connaissance approfondie de l'entité financière ainsi que du rôle du chef de l'équipe chargée du contrôle et de son positionnement stratégique, avoir l'ancienneté requise et avoir accès au conseil d'administration. Afin de réduire le risque de compromettre le TIFM, l'équipe chargée du contrôle devrait être aussi restreinte que possible.

(11) Certains éléments de risque sont inhérents aux TIFM, étant donné que des fonctions critiques sont testées dans un environnement de production réel, ce qui est susceptible de provoquer des incidents de type «déni de service», des pannes système inattendues, de dommages à des systèmes critiques en environnement de production, ou la perte, l'altération ou la divulgation de données. Ces risques mettent en évidence la nécessité de solides mesures de gestion des risques. Afin de veiller à ce que les tests d'intrusion fondés sur la menace soient conduits de manière contrôlée tout au long du processus, il est très important que les entités financières soient à tout moment conscientes des risques particuliers qu'entraîne un TIFM et que ces risques soient atténués. À cet égard, sans préjudice des processus internes de l'entité financière et de la responsabilité et des délégations déjà confiées au chef de l'équipe chargée du contrôle, des informations sur les mesures de gestion des risques liés aux TIFM ou, dans des cas particuliers, l'approbation de ces mesures par l'organe de direction de l'entité financière lui-même peuvent être appropriées. Pour être en mesure de fournir des services professionnels efficaces et hautement qualifiés et de réduire ces risques, il est également essentiel que les testeurs et les fournisseurs de renseignements sur les menaces (collectivement appelés «prestataires de TIFM») possèdent le plus haut niveau possible de compétences et d'expertise et une expérience appropriée en matière de renseignement sur les menaces et de TIFM dans le secteur des services financiers.

(12) Les tests d'intrusion conventionnels fournissent une évaluation détaillée et utile des vulnérabilités techniques et de configuration qui porte souvent sur un seul système ou environnement pris isolément, mais, contrairement aux tests de l'équipe rouge fondés sur les renseignements, ils n'évaluent pas le scénario complet d'une attaque ciblée contre une entité dans son intégralité, ce qui comprend l'ensemble de son personnel, de ses processus et de ses technologies. Au cours du processus de sélection des prestataires de TIFM, les entités financières devraient donc veiller à ce que ces derniers disposent des compétences requises pour effectuer des tests d'équipe rouge fondés sur les renseignements, et pas seulement des tests d'intrusion. Il est donc nécessaire de définir des critères complets pour les testeurs, qui peuvent être aussi bien internes qu'externes, et les fournisseurs de renseignements sur les menaces, qui sont toujours externes. Lorsque les prestataires de TIFM appartiennent à la même entreprise, le personnel affecté à un TIFM devrait être suffisamment séparé.

(13) Dans certaines circonstances exceptionnelles, il peut arriver que les entités financières ne soient pas en mesure de conclure des contrats avec des prestataires de TIFM satisfaisant à l'ensemble des critères. Dès lors qu'elles sont en mesure de prouver l'indisponibilité de tels fournisseurs de renseignements sur les menaces, les entités financières devraient être autorisées à engager des personnes qui ne satisfont pas à l'ensemble des critères, pour autant qu'elles atténuent correctement les risques supplémentaires qui en résultent et que l'autorité TIFM évalue tous ces critères.

(14) Lorsque plusieurs entités financières et plusieurs autorités TIFM sont impliquées dans un TIFM, il convient de préciser les rôles de chaque partie dans le processus de TIFM afin de garantir une efficacité et une sécurité optimales du test. Aux fins des tests groupés, des exigences spécifiques sont nécessaires pour préciser le rôle de l'entité financière désignée, à savoir qu'elle devrait être chargée de fournir toute la documentation nécessaire à l'autorité TIFM chef de file et de surveiller le processus de test. L'entité financière désignée devrait également être chargée des aspects communs de l'évaluation de la gestion des risques. Nonobstant le rôle de l'entité financière désignée, les obligations de chaque entité financière participant au processus de TIFM groupé devraient rester inchangées au cours du test groupé. Le même principe devrait s'appliquer dans le cas des TIFM communs.

(15) Comme en témoigne l'expérience acquise dans la mise en œuvre du cadre TIBER-EU, la tenue de réunions en présentiel ou virtuelles avec toutes les parties prenantes concernées (entités financières, autorités, testeurs et fournisseurs de renseignements sur les menaces) est le moyen le plus efficace de garantir la bonne conduite des tests. Des réunions en présentiel et des réunions virtuelles devraient donc avoir lieu à différentes étapes du processus, et notamment: pendant la phase de préparation lors du lancement du TIFM pour en finaliser le périmètre; pendant la phase de test pour finaliser le rapport du renseignement sur les menaces et le plan de test de l'équipe rouge et pour les mises à jour hebdomadaires; ainsi que pendant la phase de clôture pour rejouer les actions des testeurs et de l'équipe bleue, la collaboration violette et l'échange de retours d'information sur le TIFM.

(16) Afin de garantir la bonne exécution du test d'intrusion fondé sur la menace, l'autorité TIFM devrait présenter clairement à l'entité financière ses attentes en ce qui concerne le test. À cet égard, les gestionnaires de test devraient veiller à ce qu'un flux approprié d'informations soit établi avec l'équipe chargée du contrôle au sein de l'entité financière et avec les prestataires de TIFM.

(17) L'entité financière devrait sélectionner les fonctions critiques ou importantes qui entreront dans le périmètre du TIFM. Pour sélectionner ces fonctions, l'entité financière devrait se fonder sur divers critères mesurant l'importance que chacune d'entre elles revêt pour l'entité financière elle-même et pour le secteur financier, au niveau de l'Union et au niveau national, non seulement sur le plan économique, mais aussi au regard du statut symbolique ou politique de la fonction. Afin de faciliter le passage à la phase de collecte de renseignements sur les menaces, des informations détaillées sur le périmètre convenu du test devraient être fournies par l'équipe chargée du contrôle aux testeurs et aux fournisseurs de renseignements sur les menaces qui n'ont pas participé pas au processus de définition dudit périmètre.

(18) Afin de fournir aux testeurs les informations nécessaires pour simuler une attaque réelle et réaliste contre les systèmes opérationnels qui sous-tendent les fonctions critiques ou importantes de l'entité financière, le fournisseur de renseignements sur les menaces devrait recueillir des renseignements ou des informations couvrant au moins deux domaines d'intérêt clés: les cibles, par l'identification des surfaces d'attaque potentielles dans l'ensemble de l'entité financière, et les menaces, par l'identification des acteurs de la menace pertinents et des scénarios de menace probables. Afin que le fournisseur de renseignements sur les menaces tienne compte des menaces pertinentes pour l'entité financière, les testeurs, l'équipe chargée du contrôle et les gestionnaires de test devraient fournir un retour d'information sur le projet de rapport de renseignement sur les menaces. Le cas échéant, le fournisseur de renseignements sur les menaces peut utiliser un panorama général de la menace fourni par l'autorité TIFM pour le secteur financier d'un État membre en guise de référence pour le panorama national de la menace. D'après l'application du cadre TIBER-EU, le processus de collecte de renseignements sur les menaces dure généralement environ quatre semaines.

(19) Afin que les testeurs puissent se faire une idée de la situation et examiner plus en détail le document de spécification du périmètre du test ainsi que le rapport de renseignement sur les menaces ciblées pour finaliser le plan de test de l'équipe rouge, il est essentiel que, avant la phase de test de l'équipe rouge du TIFM, les testeurs reçoivent du fournisseur de renseignements sur les menaces des explications détaillées concernant le rapport de renseignement sur les menaces ciblées et une analyse des scénarios de menace possibles.

(20) Afin de permettre aux testeurs de réaliser un test réaliste et exhaustif, dans le cadre duquel toutes les phases d'attaque sont exécutées et tous les drapeaux atteints, il convient d'allouer un temps suffisant à la phase active de test de l'équipe rouge. D'après l'expérience acquise avec le cadre TIBER-EU, le délai alloué devrait être d'au moins 12 semaines et devrait être fixé en tenant compte du nombre de parties concernées, du périmètre du TIFM, des ressources de la ou des entités financières impliquées, de toute exigence externe éventuelle et de la disponibilité d'informations complémentaires fournies par l'entité financière.

(21) Au cours de la phase active de test de l'équipe rouge, les testeurs devraient déployer une série de tactiques, de techniques et de procédures pour tester de manière adéquate les systèmes en environnement de production de l'entité financière. Ces tactiques, techniques et procédures devraient inclure, le cas échéant, la reconnaissance (c'est-à-dire la collecte du plus grand nombre possible d'informations sur une cible), l'instrumentalisation (c'est-à-dire l'analyse des informations sur l'infrastructure, les installations et les employés et la préparation des opérations spécifiques à la cible), la réalisation (c'est-à-dire le lancement actif de l'opération complète sur la cible), l'exploitation (où l'objectif des testeurs est de compromettre les serveurs et les réseaux de l'entité financière et de se servir de son personnel au moyen de l'ingénierie sociale), le contrôle et le mouvement (c'est-à-dire les tentatives de passer des systèmes compromis à d'autres systèmes vulnérables ou de grande valeur) et des actions sur la cible (par exemple l'obtention d'un accès plus large aux systèmes compromis et l'obtention d'un accès à des informations et données cibles préalablement convenues, comme prévu dans le plan de test de l'équipe rouge).

(22) Lors de la réalisation d'un TIFM, les testeurs devraient agir en tenant compte du temps et des ressources dont ils disposent pour mener l'attaque, ainsi que des limites éthiques et juridiques. Si les testeurs ne sont pas en mesure de passer à l'étape suivante de l'attaque, telle que programmée, une assistance occasionnelle devrait leur être fournie par l'équipe chargée du contrôle, avec l'accord de l'autorité TIFM, sous la forme de «coups de pouce» (ou «leg-ups»). Ces coups de pouce peuvent être subdivisés grosso modo en deux catégories: «informations» et «accès». Ils peuvent ainsi consister en la fourniture d'un accès à des systèmes de TIC ou à des réseaux internes afin de permettre la poursuite du test et la préparation des étapes suivantes de l'attaque.

(23) Durant la phase active de test de l'équipe rouge, si cela est nécessaire pour permettre la poursuite du TIFM, il y a lieu de recourir à une activité de test collaborative impliquant à la fois les testeurs et l'équipe bleue. Cela ne doit toutefois se faire qu'en dernier recours, dans des circonstances exceptionnelles et une fois toutes les autres options épuisées. Dans le cadre d'un tel exercice restreint de collaboration violette, les méthodes suivantes peuvent être utilisées: le «catch-and-release» (attraper et relâcher), où les testeurs tentent de poursuivre les scénarios, se font détecter puis reprennent les tests, le «war gaming» (jeu de guerre), qui permet de mettre en œuvre des scénarios plus complexes pour tester la prise de décision stratégique, ou le «collaborative proof-of-concept» (la validation de concept collaborative), qui permet aux testeurs et aux membres de l'équipe bleue de valider conjointement des mesures, outils ou techniques de sécurité spécifiques dans un environnement contrôlé et coopératif.

(24) Le TIFM est destiné à être utilisé à des fins d'apprentissage, dans le but de renforcer la résilience opérationnelle numérique des entités financières. À ce titre, l'équipe bleue et les testeurs devraient rejouer l'attaque et revoir ensemble les mesures prises afin de tirer des enseignements du test, en collaboration avec les testeurs. Pour ce faire, et pour permettre à tous de bien se préparer, il convient, avant que les activités consistant à rejouer l'attaque ne soient menées, que les rapports de test des équipes rouge et bleue soient mis à la disposition de toutes les parties impliquées dans ces activités. En outre, au cours de la phase de clôture, il y a lieu d'organiser un exercice de collaboration violette afin de maximiser l'expérience d'apprentissage. Les méthodes à employer pour cette collaboration violette en phase de clôture devraient comprendre la discussion d'autres scénarios d'attaque, l'exploration d'autres scénarios sur les systèmes en environnement de production ou la réexploration, sur les systèmes en environnement de production, des scénarios planifiés que les testeurs n'ont pas été en mesure d'achever ou d'exécuter au cours de la phase de test.

(25) Afin de faciliter l'expérience d'apprentissage de toutes les parties impliquées dans le TIFM, dans l'optique de tests futurs, et de renforcer la résilience opérationnelle numérique des entités financières, les parties concernées devraient s'échanger des retours d'information sur l'ensemble du processus et, en particulier, pointer les activités qui se sont bien déroulées et celles qui auraient pu être améliorées, ainsi que les aspects du processus de TIFM qui ont bien fonctionné et ceux qui pourraient être améliorés.

(26) Les autorités compétentes visées à l'article 46 du règlement (UE) 2022/2554 et, si ce ne sont pas les mêmes autorités, les autorités TIFM, devraient coopérer afin d'intégrer des tests avancés dans les processus de surveillance existants, au moyen de tests d'intrusion fondés sur la menace. À cet égard, et afin de veiller à la bonne compréhension des résultats des tests d'intrusion fondés sur la menace et de la manière dont ces résultats devraient être interprétés, il convient, en particulier pour le rapport de synthèse des tests et les plans de mesures correctives, qu'une coopération étroite soit établie entre les gestionnaires de test qui ont participé au TIFM et les autorités de surveillance responsables.

(27) L'article 26, paragraphe 8, premier alinéa, du règlement (UE) 2022/2554 impose aux entités financières d'engager des testeurs externes tous les trois tests. Lorsque les entités financières incluent dans l'équipe de testeurs à la fois des testeurs internes et externes, le TIFM doit être considéré, aux fins dudit article, comme effectué avec des testeurs internes.

(28) Le présent règlement se fonde sur le projet de normes techniques de réglementation soumis à la Commission par l'Autorité bancaire européenne, l'Autorité européenne des assurances et des pensions professionnelles et l'Autorité européenne des marchés financiers (les «autorités européennes de surveillance»), en accord avec la Banque centrale européenne.

(29) Les autorités européennes de surveillance ont procédé à des consultations publiques ouvertes sur le projet de normes techniques de réglementation sur lequel se fonde le présent règlement, analysé les coûts et avantages potentiels qu'il implique et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué en application de l'article 37 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil ([3]), du groupe des parties intéressées à l'assurance et la réassurance et du groupe des parties intéressées aux pensions professionnelles institués en application de l'article 37 du règlement (UE) nº 1094/2010 du Parlement européen et du Conseil ([4]) et du groupe des parties intéressées au secteur financier institué en application de l'article 37 du règlement (UE) nº 1095/2010 du Parlement européen et du Conseil ([5]).

(30) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et a rendu un avis le 20 août 2024,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article 1

Définitions

Aux fins du présent règlement, on entend par:

1) «équipe chargée du contrôle»: l'équipe qui est composée de membres du personnel de l'entité financière testée et, si cela est pertinent au regard du périmètre du test d'intrusion fondé sur la menace (TIFM), de membres du personnel de ses prestataires tiers de services et de toute autre partie, et qui gère le test;

2) «chef de l'équipe chargée du contrôle»: le membre du personnel de l'entité financière qui est responsable de la conduite de toutes les activités liées aux tests d'intrusion fondés sur la menace (TIFM) pour l'entité financière dans le cadre d'un test donné;

3) «équipe bleue»: les membres du personnel de l'entité financière et, le cas échéant, les membres du personnel des prestataires tiers de services de l'entité financière et de toute autre partie jugée pertinente au regard du périmètre du test d'intrusion fondé sur la menace (TIFM), des prestataires tiers de services de l'entité financière, qui défendent l'utilisation des réseaux et des systèmes d'information par une entité financière en maintenant sa posture de sécurité face aux attaques simulées ou réelles et qui n'ont pas connaissance du TIFM;

4) «tâches d'équipe bleue»: les tâches qui sont généralement exécutées par l'équipe bleue, telles que le centre d'opérations de sécurité (SOC), les services d'infrastructure TIC, les services d'assistance et les services de gestion des incidents au niveau opérationnel;

5) «équipe rouge»: les testeurs, internes ou externes, affectés à, ou engagés pour, un test d'intrusion fondé sur la menace (TIFM);

6) «collaboration violette»: une activité de test collaborative impliquant à la fois les testeurs et l'équipe bleue;

([3]) Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Règlement (UE) nº 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission (JO L 331 du 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) «autorité compétente en matière de tests d'intrusion fondés sur la menace» ou «autorité TIFM»: l'une des entités suivantes:

   a) l'autorité publique unique au sein du secteur financier désignée conformément à l'article 26, paragraphe 9, du règlement (UE) 2022/2554;

   b) l'autorité du secteur financier à laquelle l'exercice de tout ou partie des tâches liées aux tests d'intrusion fondés sur la menace (TIFM) est délégué conformément à l'article 26, paragraphe 10, du règlement (UE) 2022/2554;

   c) l'une des autorités compétentes visées à l'article 46 du règlement (UE) 2022/2554;

8) «équipe de cybersécurité TIFM»: les membres du personnel qui, au sein des autorités TIFM, sont responsables des questions liées aux tests d'intrusion fondés sur la menace (TIFM);

9) «gestionnaires de test»: les membres du personnel désignés pour diriger les activités de l'autorité TIFM pour un test d'intrusion fondé sur la menace (TIFM) spécifique afin de contrôler le respect du présent règlement;

10) «fournisseur de renseignements sur les menaces»: les experts qui sont engagés par l'entité financière pour chaque test d'intrusion fondé sur la menace (TIFM) et sont externes à l'entité financière et aux éventuels prestataires de services TIC intra-groupe, et qui collectent et analysent des renseignements sur les menaces ciblées pertinents pour les entités financières dans le périmètre d'un exercice spécifique de TIFM et élaborent des scénarios de menace correspondants pertinents et réalistes;

11) «prestataires de TIFM»: les testeurs et les fournisseurs de renseignements sur les menaces;

12) «coup de pouce»: l'assistance ou les informations fournies par l'équipe chargée du contrôle aux testeurs pour leur permettre de poursuivre l'exécution d'un chemin d'attaque lorsqu'ils ne sont pas en mesure de continuer seuls, notamment par manque de temps ou de ressources lors d'un test d'intrusion fondé sur la menace (TIFM) donné, et qu'il n'existe pas d'autre solution raisonnable;

13) «chemin d'attaque»: la voie suivie par les testeurs au cours de la phase active de test de l'équipe rouge, lors d'un test d'intrusion fondé sur la menace (TIFM), pour atteindre les drapeaux spécifiés pour ce test;

14) «drapeaux»: des objectifs clés dans les systèmes de TIC soutenant les fonctions critiques ou importantes d'une entité financière que les testeurs tentent d'atteindre dans le cadre du test;

15) «informations sensibles»: des informations qui peuvent facilement être exploitées pour mener des attaques contre les systèmes de TIC de l'entité financière, la propriété intellectuelle, des données commerciales confidentielles ou des données à caractère personnel, qui, si elles tombaient entre les mains d'acteurs malveillants, pourraient porter directement ou indirectement préjudice à l'entité financière et à son écosystème;

16) «groupement»: toutes les entités financières participant à un test groupé d'intrusion fondé sur la menace (TIFM groupé) conformément à l'article 26, paragraphe 4, du règlement (UE) 2022/2554;

17) «État membre d'accueil»: l'État membre d'accueil conformément au droit sectoriel de l'Union applicable à chaque entité financière;

18) «test commun d'intrusion fondé sur la menace» ou «TIFM commun»: un test d'intrusion fondé sur la menace (TIFM), autre qu'un test groupé d'intrusion fondé sur la menace (TIFM groupé) au sens de l'article 26, paragraphe 4, du règlement (UE) 2022/2554, impliquant plusieurs entités financières utilisant le même prestataire de services TIC intra-groupe, ou appartenant à un même groupe et partageant des systèmes de TIC.

Article 2

Identification des entités financières tenues d'effectuer des TIFM

1. Les autorités TIFM évaluent si une entité financière est tenue d'effectuer des TIFM, en tenant compte de l'incidence de cette entité financière, de son caractère systémique et de son profil de risque lié aux TIC, sur la base de l'ensemble des critères suivants:

a) facteurs liés à l'incidence et au caractère systémique:

   i) la taille de l'entité financière, déterminée en examinant si l'entité financière fournit des services financiers dans un seul État membre ou dans plusieurs et en comparant les activités de l'entité financière à celles d'autres entités financières fournissant des services similaires;

   ii) l'ampleur et la nature de l'interconnexion de l'entité financière avec d'autres entités financières du secteur financier dans un ou plusieurs États membres;

   iii) la criticité ou l'importance des services que l'entité financière fournit au secteur financier;

iv) la substituabilité des services fournis par l'entité financière;

v) la complexité du modèle économique de l'entité financière et des services et processus connexes;

vi) le fait que l'entité financière fasse ou non partie d'un groupe de caractère systémique au niveau de l'Union ou au niveau national dans le secteur financier qui partage des systèmes de TIC;

b) facteurs liés aux risques liés aux TIC:

i) le profil de risque de l'entité financière;

ii) le panorama de la menace relatif à l'entité financière;

iii) le degré de dépendance des fonctions critiques ou importantes de l'entité financière, ou de leurs fonctions de soutien, à l'égard des systèmes et processus de TIC;

iv) la complexité de l'architecture des TIC de l'entité financière;

v) les services et fonctions de TIC soutenus par des prestataires tiers de services TIC, ainsi que le nombre et le type d'accords contractuels conclus avec des prestataires tiers de services TIC ou des prestataires de services TIC intra-groupe;

vi) les résultats des examens des autorités de surveillance pertinents pour l'évaluation de la maturité des TIC de l'entité financière;

vii) la maturité des plans de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC;

viii) la maturité des mesures opérationnelles de détection et d'atténuation en matière de sécurité des TIC, y compris la capacité:

1) d'assurer une surveillance permanente de l'infrastructure TIC de l'entité financière;

2) de détecter les événements liés aux TIC en temps réel;

3) d'analyser les événements visés au point 2);

4) de réagir aux événements visés au point 2) en temps utile et de manière efficace;

ix) le fait que l'entité financière fasse ou non partie d'un groupe actif dans le secteur financier au niveau de l'Union ou au niveau national qui partage des systèmes de TIC.

Aux fins du point a), i), l'autorité TIFM tient compte, dans la mesure du possible:

a) de la part de marché de l'entité financière au niveau de l'Union et au niveau national;

b) de l'éventail des activités proposées par l'entité financière;

c) de la part de marché des services fournis par l'entité financière ou des activités menées au niveau de l'Union et au niveau national.

Aux fins du point a), v), l'autorité TIFM tient compte, dans la mesure du possible:

a) du fait que l'entité financière applique ou non plus d'un modèle d'entreprise;

b) de l'interconnexion des différents processus opérationnels et des services connexes.

2. Les autorités TIFM exigent de toutes les entités financières suivantes qu'elles effectuent des TIFM à moins que l'évaluation visée au paragraphe 1 n'indique, en ce qui concerne une entité financière, que son incidence, les préoccupations relatives à la stabilité financière qui lui sont liées, ou son profil de risque lié aux TIC ne justifient pas la réalisation d'un TIFM:

a) les établissements de crédit qui remplissent l'une des conditions suivantes:

i) ils ont été recensés comme établissements d'importance systémique mondiale (EISm) conformément à l'article 131 de la directive 2013/36/UE du Parlement européen et du Conseil ([7]);

ii) ils ont été recensés comme autres établissements d'importance systémique (autres EIS) conformément à l'article 131 de la directive 2013/36/UE;

iii) ils font partie d'un EISm ou d'un autre EIS;

([7]) Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) les établissements de paiement qui ont dépassé, au cours de chacune des deux années civiles précédant l'évaluation effectuée par l'autorité TIFM, la barre des 150 milliards d'EUR en valeur totale des opérations de paiement au sens de l'article 4, point 5), de la directive (UE) 2015/2366 du Parlement européen et du Conseil ([8]);

c) les établissements de monnaie électronique qui ont dépassé, au cours de chacune des deux années civiles précédant l'évaluation effectuée par l'autorité TIFM, soit la barre des 150 milliards d'EUR en valeur totale des opérations de paiement au sens de l'article 4, point 5), de la directive (UE) 2015/2366, soit la barre des 40 milliards d'EUR en valeur totale de la monnaie électronique en circulation;

d) les dépositaires centraux de titres;

e) les contreparties centrales;

f) les plates-formes de négociation dotées d'un système de négociation électronique qui remplissent l'un des critères suivants:

i) la plate-forme de négociation détient, au cours de chacune des deux années civiles précédant l'évaluation effectuée par l'autorité TIFM, la part de marché la plus élevée en termes de volume d'échanges au niveau national dans l'une des catégories suivantes:

1) valeurs mobilières au sens de l'article 4, paragraphe 1, point 44), a), de la directive 2014/65/UE du Parlement européen et du Conseil ([9]);

2) valeurs mobilières au sens de l'article 4, paragraphe 1, point 44), b), de la directive 2014/65/UE;

3) instruments dérivés au sens de l'article 2, paragraphe 1, point 29), du règlement (UE) nº 600/2014 du Parlement européen et du Conseil ([10]);

4) produits financiers structurés au sens de l'article 2, paragraphe 1, point 28), du règlement (UE) nº 600/2014;

5) quotas d'émission visés à l'annexe I, section C, point 11), de la directive 2014/65/UE;

ii) la plate-forme de négociation détient, au cours de chacune des deux années civiles précédant l'évaluation effectuée par l'autorité TIFM, une part de marché en termes de volume d'échanges au niveau de l'Union qui dépasse 5 % dans l'une des catégories suivantes:

1) actions de sociétés et autres titres équivalents à des actions de sociétés, de sociétés de type partnership ou d'autres entités ainsi que certificats représentatifs d'actions;

2) obligations et autres titres de créance, y compris certificats représentatifs de tels titres;

3) instruments dérivés au sens de l'article 2, paragraphe 1, point 29), du règlement (UE) nº 600/2014;

4) produits financiers structurés au sens de l'article 2, paragraphe 1, point 28), du règlement (UE) nº 600/2014;

5) quotas d'émission visés à l'annexe I, section C, point 11), de la directive 2014/65/UE;

([8]) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) les entreprises d'assurance et de réassurance qui remplissent tous les critères suivants:

i) leur montant de primes brutes émises est supérieur à 1 500 000 000 EUR;

ii) leur montant de provisions techniques est supérieur à 10 000 000 000 EUR;

iii) ce sont des entreprises d'assurance qui exercent uniquement des activités vie ou qui exercent à la fois des activités vie et non-vie et dont le total des actifs dépasse 3,5 % de la somme du total des actifs des entreprises d'assurance et de réassurance établies dans l'État membre, valorisés conformément à l'article 75 de la directive 2009/138/CE du Parlement européen et du Conseil ([11]).

Aux fins du point f), ii), lorsque la plate-forme de négociation fait partie d'un groupe partageant des systèmes de TIC ou le même prestataire de services TIC intra-groupe, le volume d'échanges des titres et des contrats dérivés sur l'ensemble des plates-formes de négociation appartenant au même groupe et établies dans l'Union est pris en considération.

Aux fins du point g), les autorités TIFM identifient un sous-ensemble de toutes les entreprises d'assurance et de réassurance en appliquant les critères énoncés au point g), i), ii) et iii). Les entreprises d'assurance et de réassurance incluses dans ce sous-ensemble sont tenues d'effectuer des TIFM lorsqu'elles remplissent également l'un des critères suivants:

a) montant de primes brutes émises supérieur à 3 000 000 000 EUR;

b) montant de provisions techniques supérieur à 30 000 000 000 EUR;

c) total des actifs qui dépasse 10 % de la somme du total des actifs des entreprises d'assurance et de réassurance établies dans l'État membre, valorisés conformément à l'article 75 de la directive 2009/138/CE.

3. Lorsque plusieurs entités financières appartenant au même groupe et partageant des systèmes de TIC, ou plusieurs entités financières ayant recours au même prestataire de services TIC intra-groupe, remplissent les critères énoncés au paragraphe 2, les autorités TIFM de ces entités financières décident, conformément à l'article 16, paragraphe 2, si l'exigence d'effectuer des TIFM sur une base individuelle est pertinente pour lesdites entités financières.

Lorsque l'autorité TIFM de l'entreprise mère d'un groupe d'entités financières visée au premier alinéa est différente des autorités TIFM des entités financières du groupe, cette autorité est consultée par les autorités TIFM des entités financières appartenant à ce groupe quant à l'opportunité d'effectuer des TIFM sur une base individuelle.

Article 3

Équipe de cybersécurité TIFM et gestionnaires de test TIFM

1. Une autorité TIFM confie à une équipe de cybersécurité TIFM la responsabilité de coordonner les activités liées aux TIFM. Cette équipe est composée de gestionnaires de test chargés de superviser un TIFM individuel.

2. Pour chaque test, l'autorité TIFM désigne un gestionnaire de test et au moins un suppléant.

3. Les gestionnaires de test vérifient si les exigences énoncées dans le présent règlement sont respectées et ils font en sorte qu'elles le soient.

([11]) Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (JO L 335 du 17.12.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Le gestionnaire de test communique les coordonnées de l'équipe de cybersécurité TIFM à l'entité financière au moyen de la notification visée à l'article 9, paragraphe 1.

5. L'autorité TIFM participe à toutes les phases du TIFM.

Article 4

Modalités organisationnelles pour les entités financières

1. Les entités financières désignent un chef pour l'équipe chargée du contrôle, auquel incombe la responsabilité de la gestion journalière du TIFM ainsi que des décisions et actions de l'équipe chargée du contrôle.

2. Les entités financières établissent des mesures organisationnelles et procédurales pour faire en sorte que:

a) l'accès aux informations relatives à tout TIFM prévu ou en cours soit réservé, sur la base du besoin d'en connaître, à l'équipe chargée du contrôle, à l'organe de direction, aux testeurs, au fournisseur de renseignements sur les menaces et à l'autorité TIFM;

b) l'équipe chargée du contrôle consulte les gestionnaires de test avant d'associer tout membre de l'équipe bleue à un TIFM;

c) l'équipe chargée du contrôle soit informée de toute détection du TIFM par des membres du personnel de l'entité financière ou de ses prestataires tiers de services; en cas de remontée de la réponse à l'incident qui en résulte, si nécessaire, l'équipe chargée du contrôle bloque cette remontée;

d) des dispositions relatives à la confidentialité du TIFM, applicables au personnel de l'entité financière, au personnel des prestataires tiers de services TIC concernés, aux testeurs et au fournisseur de renseignements sur les menaces, soient en place;

e) sur demande, l'équipe chargée du contrôle fournisse aux gestionnaires de test toutes les informations relatives au TIFM;

f) dans la mesure du possible, les parties impliquées dans le TIFM ne fassent référence à ce dernier que par son nom de code.

Article 5

Gestion des risques pour les TIFM

1. Au cours de la phase de préparation visée à l'article 9, l'équipe chargée du contrôle évalue les risques associés au test des systèmes en environnement de production des fonctions critiques ou importantes de l'entité financière, y compris les incidences potentielles sur:

a) le secteur financier;

b) la stabilité financière au niveau de l'Union ou au niveau national.

L'équipe chargée du contrôle examine ces incidences tout au long des tests.

2. Aux fins de l'évaluation et de la gestion des risques, l'équipe chargée du contrôle tient compte au moins des types de risques suivants liés:

a) au fait d'accorder au fournisseur de renseignements sur les menaces et aux testeurs externes, le cas échéant, l'accès à des informations sensibles sur l'entité financière;

b) au non-respect, par le TIFM, du règlement (UE) 2022/2554 et du présent règlement lorsque ce non-respect entraîne l'absence de l'attestation visée à l'article 26, paragraphe 7, du règlement (UE) 2022/2554, y compris lorsque ce non-respect est dû à des violations de la confidentialité du TIFM ou à une conduite non éthique;

c) à une remontée des incidents et des crises;

d) à la phase active de l'équipe rouge, en ce compris les risques liés à l'interruption d'activités critiques et à la corruption de données due aux activités des testeurs, et à ses incidences potentielles sur des tiers;

e) à l'activité de l'équipe bleue, en ce compris les risques liés à l'interruption d'activités critiques et à la corruption de données due aux activités de l'équipe bleue, et à ses incidences potentielles sur des tiers;

f) à la restauration incomplète des systèmes touchés par le TIFM.

Article 6

Gestion des risques pour les TIFM groupés ou communs d'intrusion fondés sur la menace

1. Dans le cas d'un TIFM commun ou d'un TIFM groupé, l'équipe chargée du contrôle de chaque entité financière procède à sa propre évaluation des risques et établit ses propres mesures de gestion des risques.

2. L'équipe chargée du contrôle de l'entité financière désignée visée à l'article 16, paragraphe 3, point b), du présent règlement, ou de l'entité financière désignée conformément à l'article 26, paragraphe 4, du règlement (UE) 2022/2554, évalue les risques liés à la participation de plusieurs entités financières au TIFM. Les équipes chargées du contrôle des entités financières impliquées coopèrent avec l'équipe chargée du contrôle de l'entité financière désignée afin d'identifier les risques communs potentiels.

Article 7

Sélection des prestataires de TIFM

1. L'équipe chargée du contrôle prend des mesures pour gérer les risques liés aux TIFM et veille en particulier à ce que, pour chaque TIFM:

a) le fournisseur de renseignements sur les menaces et les testeurs externes fournissent à l'équipe chargée du contrôle un curriculum vitæ détaillé et des copies de certifications qui, selon les normes du marché reconnues, sont adaptées à l'exercice de leurs activités;

b) le fournisseur de renseignements sur les menaces et le testeur externe soient dûment et entièrement couverts par des assurances de responsabilité civile professionnelle adéquates, y compris contre les risques de mauvaise conduite et de négligence;

c) le fournisseur de renseignements sur les menaces fournisse au moins trois références issues de missions antérieures dans le cadre de tests d'intrusion et de tests par équipe rouge;

d) les testeurs externes fournissent au moins cinq références issues de missions antérieures liées à des tests d'intrusion et à des tests par équipe rouge;

e) le personnel du fournisseur de renseignements sur les menaces affecté au TIFM:

   i) soit composé d'au moins un cadre possédant un minimum de cinq années d'expérience dans le domaine du renseignement sur les menaces et d'au moins un autre membre ayant un minimum de deux ans d'expérience dans le domaine du renseignement sur les menaces;

   ii) présente un large éventail de connaissances et de compétences professionnelles d'un niveau approprié, notamment dans les domaines suivants:

      1) tactiques, techniques et procédures de collecte de renseignements;

      2) connaissances géopolitiques, techniques et sectorielles;

      3) compétences adéquates en matière de communication pour présenter clairement les résultats de l'engagement et en rendre compte;

   iii) ait déjà participé, si l'on considère la participation combinée de ses membres, à au moins trois missions de renseignement sur les menaces dans le cadre de tests d'intrusion et de tests par équipe rouge;

   iv) n'exécute pas simultanément des tâches d'équipe bleue ou d'autres services susceptibles de présenter un conflit d'intérêts en ce qui concerne l'entité financière, le prestataire tiers de services TIC ou un prestataire de services TIC intra-groupe participant au TIFM auquel il est affecté;

   v) soit séparé du personnel du même prestataire de TIFM qui fournit des testeurs externes pour le même TIFM, et ne rende pas compte à celui-ci;

f) pour les testeurs externes, l'équipe rouge affectée au TIFM:

i) soit composée d'au moins un cadre possédant un minimum de cinq années d'expérience dans les tests d'intrusion et les tests par équipe rouge, ainsi que d'au moins deux autres testeurs ayant chacun un minimum de deux ans d'expérience dans les tests d'intrusion et les tests par équipe rouge;

ii) présente un large éventail de connaissances et de compétences professionnelles d'un niveau approprié, y compris des connaissances sur l'activité de l'entité financière, la reconnaissance, la gestion des risques, le développement d'exploit, l'intrusion physique, l'ingénierie sociale, l'analyse de vulnérabilité, ainsi que des compétences adéquates en matière de communication afin de présenter clairement les résultats de l'engagement et d'en rendre compte;

iii) ait déjà participé, si l'on considère la participation combinée de ses membres, à au moins cinq missions liées à des tests d'intrusion et à des tests par équipe rouge;

iv) ne soit pas employée par un fournisseur de renseignements sur les menaces qui exécute simultanément des tâches d'équipe bleue pour une entité financière, un prestataire tiers de services TIC ou un prestataire de services TIC intra-groupe qui participe au TIFM, ni ne fournisse de services à ce fournisseur de renseignements sur les menaces;

v) soit séparée de tout membre du personnel du même prestataire de TIFM qui fournit simultanément des services de renseignement sur les menaces pour le même TIFM;

g) les testeurs et le fournisseur de renseignements sur les menaces mettent en œuvre des procédures de restauration à l'issue des tests, lesquelles comprennent la suppression sécurisée des informations relatives aux mots de passe, aux identifiants et aux autres clés secrètes compromises durant le TIFM, la communication sécurisée aux entités financières des comptes compromis, la collecte, le stockage, la gestion et l'élimination sécurisés d'autres données collectées au cours des tests;

h) outre les procédures de restauration à l'issue des tests visées au point g), les testeurs effectuent les procédures de restauration suivantes:

i) la désactivation des commandes et contrôles;

ii) la mise en place de coupe-circuit («kill switch») assortis d'une date et d'un périmètre;

iii) l'élimination des portes dérobées («backdoor») et autres logiciels malveillants;

iv) la notification des violations potentielles;

v) les procédures de restauration de sauvegarde future qui pourraient concerner des logiciels malveillants ou des outils installés au cours du test;

vi) le suivi des activités de l'équipe bleue et la notification de toute détection éventuelle à l'équipe chargée du contrôle;

i) les testeurs et le fournisseur de renseignements sur les menaces n'exercent aucune des activités suivantes ni n'y participent:

i) la destruction non autorisée d'équipements de l'entité financière et de ses éventuels prestataires tiers de services TIC;

ii) la modification incontrôlée d'actifs informationnels et d'actifs de TIC de l'entité financière et de ses éventuels prestataires tiers de services TIC;

iii) la compromission intentionnelle de la continuité de fonctions critiques ou importantes de l'entité financière;

iv) l'inclusion non autorisée de systèmes situés hors du périmètre du test;

v) la divulgation non autorisée des résultats des tests.

2. L'équipe chargée du contrôle tient un registre de la documentation fournie par les testeurs et les fournisseurs de renseignements sur les menaces afin de prouver le respect du paragraphe 1, points a) à f).

Dans des circonstances exceptionnelles, les entités financières peuvent faire appel à des testeurs externes et à des fournisseurs de renseignements sur les menaces qui ne satisfont pas à une ou à plusieurs des exigences énoncées au paragraphe 1, points a) à f), à condition que ces entités financières adoptent des mesures appropriées pour atténuer les risques liés au non-respect de ces points et consignent ces mesures.

Article 8

Spécificités des TIFM groupés ou communs

1. Sauf décision contraire de l'autorité TIFM chef de file, lorsque plusieurs entités financières, identifiées conformément à l'article 16, paragraphe 2 ou 4, participent à un TIFM groupé ou commun, chaque entité financière suit chacune des étapes énoncées aux articles 9 à 15.

2. Sauf disposition contraire du présent règlement, lorsque plusieurs autorités TIFM participent à un TIFM commun ou à un TIFM groupé, au sens de l'article 16, paragraphe 3 ou 5, les références à l'«autorité TIFM» faites aux articles 9 à 15 s'entendent comme une référence à l'autorité TIFM chef de file pour ces TIFM groupés ou communs.

Article 9

Phase de préparation

1. Une entité financière identifiée conformément à l'article 26, paragraphe 8, troisième alinéa, du règlement (UE) 2022/2554 lance un TIFM à la suite d'une notification reçue de l'autorité TIFM indiquant qu'un TIFM doit être effectué.

2. Dans un délai de trois mois à compter de la réception de la notification visée au paragraphe 1, l'entité financière communique aux gestionnaires de test toutes les informations suivantes concernant le lancement du TIFM:

a) une charte de projet comprenant un plan de projet de haut niveau, contenant les informations visées à l'annexe I;

b) les coordonnées du chef de l'équipe chargée du contrôle;

c) des informations sur le recours prévu à des testeurs internes ou externes, ou les deux, le cas échéant, comme indiqué à l'article 15;

d) des informations sur les canaux de communication à utiliser pendant le TIFM;

e) le nom de code du TIFM.

3. Lorsque les informations visées au paragraphe 2, points a) à e), sont complètes et garantissent l'adéquation et l'exécution effective du TIFM, l'autorité TIFM valide les informations relatives au lancement du TIFM de l'entité financière et en informe celle-ci.

4. À la suite de la validation, par l'autorité TIFM, des informations relatives au lancement du TIFM, l'entité financière met en place une équipe chargée du contrôle afin d'assister le chef de l'équipe chargée du contrôle dans ses tâches consistant à:

a) définir les canaux et processus de communication au sein de l'équipe chargée du contrôle, avec les testeurs et les fournisseurs de renseignements sur les menaces pour toutes les questions liées au TIFM;

b) informer l'organe de direction de l'entité financière de l'état d'avancement du TIFM et des risques associés;

c) prendre des décisions fondées sur l'expertise en la matière tout au long du TIFM;

d) exécuter le TIFM conformément au présent règlement;

e) sélectionner le fournisseur de renseignements sur les menaces pour le TIFM;

f) sélectionner les testeurs externes, les testeurs internes ou les deux;

g) préparer le document de spécification du périmètre du test.

5. Lorsque l'autorité TIFM estime que la composition initiale de l'équipe chargée du contrôle et toute modification ultérieure apportée à celle-ci sont adéquates pour l'exécution des tâches visées au paragraphe 4, elle valide l'équipe chargée du contrôle et le notifie au chef de l'équipe.

6. Dans un délai de six mois à compter de la réception de la notification de l'autorité TIFM visée au paragraphe 1, l'entité financière soumet aux gestionnaires de test un document de spécification du périmètre du test contenant toutes les informations prévues à l'annexe II. L'organe de direction de l'entité financière approuve le document de spécification du périmètre du test.

7. Les entités financières prennent en considération les critères suivants pour l'inclusion de fonctions critiques ou importantes dans le périmètre du TIFM:

a) la criticité ou l'importance de la fonction et son incidence possible sur le secteur financier et sur la stabilité financière au niveau de l'Union et au niveau national;

b) l'importance de la fonction pour les opérations courantes de l'entité financière;

c) l'interchangeabilité de la fonction;

d) l'interconnexion avec d'autres fonctions;

e) la localisation géographique de la fonction;

f) la dépendance sectorielle d'autres entités à l'égard de la fonction;

g) le cas échéant, des renseignements sur les menaces concernant la fonction.

8. L'équipe chargée du contrôle partage les informations relatives au lancement du TIFM ainsi que le document de spécification du périmètre du test avec les testeurs et les fournisseurs de renseignements sur les menaces une fois ceux-ci engagés. L'équipe chargée du contrôle informe les testeurs et les fournisseurs de renseignements sur les menaces de la procédure à suivre pour le test.

9. L'entité financière veille à ce que le recrutement ou l'affectation de testeurs et de fournisseurs de renseignements sur les menaces soit achevé(e) avant le début de la phase de test.

10. Avant le début de la phase de test, l'équipe chargée du contrôle consulte les gestionnaires de test sur l'évaluation des risques liés aux TIFM et sur les mesures de gestion des risques. L'équipe chargée du contrôle réexamine l'évaluation des risques ou les mesures de gestion des risques lorsque l'autorité TIFM estime qu'elles ne tiennent pas compte de manière adéquate des risques liés aux TIFM.

11. L'équipe chargée du contrôle évalue le respect, par les fournisseurs de renseignements sur les menaces et les testeurs qu'elle envisage d'associer au TIFM, des exigences énoncées à l'article 27 du règlement (UE) 2022/2554 et des dispositions de l'article 7, paragraphe 1, du présent règlement, et documente les résultats de cette évaluation. L'équipe chargée du contrôle sélectionne les fournisseurs de renseignements sur les menaces conformément à cette évaluation et à ses pratiques de gestion des risques. Avant de conclure un contrat avec les fournisseurs de renseignements sur les menaces et les testeurs externes sélectionnés, l'équipe chargée du contrôle fournit aux gestionnaires de test la preuve que ces fournisseurs de renseignements sur les menaces et ces testeurs respectent les exigences énoncées à l'article 27 du règlement (UE) 2022/2554 et les dispositions de l'article 7, paragraphe 1, du présent règlement. L'équipe chargée du contrôle ne procède pas à la passation de contrats avec les fournisseurs de renseignements sur les menaces et les testeurs externes sélectionnés si l'autorité TIFM estime que ceux-ci ne respectent pas les exigences énoncées à l'article 27 du règlement (UE) 2022/2554, les exigences énoncées à l'article 7, paragraphe 1, du présent règlement ou des exigences supplémentaires découlant des législations nationales en matière de sécurité conformément au droit de l'Union, ou si l'entité financière ne respecte pas les dispositions de l'article 7, paragraphe 2, premier alinéa, du présent règlement, ou encore si les conditions visées à l'article 7, paragraphe 2, deuxième alinéa, du présent règlement ne sont pas réunies.

12. Lorsque le document de spécification du périmètre du test est complet et garantit la réalisation d'un TIFM approprié et efficace, l'autorité TIFM approuve ce document et en informe le chef de l'équipe chargée du contrôle.

Article 10

Phase de test: renseignements sur les menaces

1. À la suite de l'approbation du document de spécification du périmètre du test par l'autorité TIFM, le fournisseur de renseignements sur les menaces analyse les renseignements sur les menaces génériques et sectoriels pertinents pour l'entité financière. Lorsqu'un panorama générique de la menace a été fourni par l'autorité TIFM pour le secteur financier d'un État membre, le fournisseur de renseignements sur les menaces peut l'utiliser en guise de référence pour le panorama national de la menace. Le fournisseur de renseignements sur les menaces recense les cybermenaces et les vulnérabilités existantes ou potentielles concernant l'entité financière. En outre, il recueille des informations et analyse des renseignements concrets, exploitables et contextualisés sur les cibles et les menaces concernant l'entité financière, y compris en consultant l'équipe chargée du contrôle et les gestionnaires de test.

2. Le fournisseur de renseignements sur les menaces présente les menaces pertinentes et les renseignements sur les menaces ciblées et propose les scénarios requis à l'équipe chargée du contrôle, aux testeurs et aux gestionnaires de test. Les scénarios proposés diffèrent en fonction des acteurs de la menace identifiés et des tactiques, techniques et procédures associées et ciblent chacune des fonctions critiques ou importantes incluses dans le périmètre du TIFM.

3. Le chef de l'équipe chargée du contrôle sélectionne au moins trois scénarios pour réaliser le TIFM sur la base de tous les éléments suivants:

a) la recommandation du fournisseur de renseignements sur les menaces et la nature, axée sur les menaces, de chaque scénario;

b) les contributions fournies par les gestionnaires de test;

c) la faisabilité de l'exécution des scénarios proposés, sur la base du jugement d'expert des testeurs;

d) la taille, la complexité et le profil de risque global de l'entité financière ainsi que la nature, l'ampleur et la complexité de ses services, activités et opérations.

4. Seul un des scénarios sélectionnés peut ne pas être fondé sur la menace et peut être fondé sur une menace prospective et potentiellement fictive présentant une valeur prédictive, anticipative, opportuniste ou prospective élevée, compte tenu de l'évolution attendue du panorama de la menace concernant l'entité financière.

Pour les TIFM groupés, sans préjudice des scénarios ciblant directement les fonctions critiques ou importantes des entités financières participant aux tests, au moins un scénario inclut les systèmes, processus et technologies de TIC sous-jacents pertinents du prestataire tiers de services TIC qui soutiennent les fonctions critiques ou importantes des entités financières incluses dans le périmètre.

Lorsque le test est un TIFM commun impliquant un prestataire de services TIC intra-groupe, sans préjudice des scénarios ciblant directement les fonctions critiques ou importantes des entités financières participant au test, au moins un scénario inclut les systèmes, processus et technologies de TIC sous-jacents pertinents du prestataire de services TIC intra-groupe qui soutiennent les fonctions critiques ou importantes des entités financières incluses dans le périmètre.

5. Le fournisseur de renseignements sur les menaces fournit le rapport de renseignement sur les menaces ciblées à l'équipe chargée du contrôle, en ce compris les scénarios sélectionnés conformément aux paragraphes 3 et 4. Le rapport de renseignement sur les menaces contient les informations prévues à l'annexe III.

6. L'équipe chargée du contrôle soumet le rapport de renseignement sur les menaces ciblées au gestionnaire de test pour approbation. Lorsque le rapport de renseignement sur les menaces ciblées est complet et garantit la réalisation d'un TIFM efficace, l'autorité du TIFM l'approuve et en informe le chef de l'équipe chargée du contrôle.

Article 11

Phase de test: test de l'équipe rouge

1. Après l'approbation, par l'autorité TIFM, du rapport de renseignement sur les menaces ciblées, les testeurs élaborent le plan de test de l'équipe rouge, qui contient les informations prévues à l'annexe IV. Les testeurs utilisent le document de spécification du périmètre du test et le rapport de renseignement sur les menaces ciblées pour produire les scénarios d'attaque.

2. Les testeurs consultent l'équipe chargée du contrôle, le fournisseur de renseignements sur les menaces et les gestionnaires de test au sujet du plan de test de l'équipe rouge, en ce compris les modalités de communication, de procédure et de gestion de projet, la préparation et les cas d'utilisation pour l'activation des coups de pouce, ainsi que les arrangements relatifs aux rapports à présenter à l'équipe chargée du contrôle et aux gestionnaires de test.

3. Lorsque le plan de test de l'équipe rouge est complet et garantit la réalisation d'un TIFM efficace, l'équipe chargée du contrôle et l'autorité TIFM l'approuvent et en informent le chef de l'équipe chargée du contrôle.

4. Après approbation du plan de test de l'équipe rouge conformément au paragraphe 3, les testeurs effectuent le TIFM pendant la phase active de test de l'équipe rouge.

5. La durée de la phase active de test de l'équipe rouge est proportionnée au périmètre du TIFM ainsi qu'à l'échelle, à l'activité, à la complexité et au nombre des entités financières et des prestataires de services TIC tiers ou intra-groupe participant au TIFM et elle est, en tout état de cause, d'au moins 12 semaines. Les scénarios d'attaque peuvent être exécutés successivement ou simultanément. L'équipe chargée du contrôle, le fournisseur de renseignements sur les menaces, les testeurs et les gestionnaires de test conviennent de la fin de la phase active de test de l'équipe rouge.

6. À condition que le plan de test de l'équipe rouge reste complet et permette la réalisation d'un TIFM efficace, le chef de l'équipe chargée du contrôle et les gestionnaires de test approuvent toute modification apportée au plan de test de l'équipe rouge après son approbation, y compris en ce qui concerne son calendrier, son périmètre, ses systèmes cibles ou ses drapeaux.

7. Tout au long de la phase active de test de l'équipe rouge, les testeurs rendent compte au moins une fois par semaine à l'équipe chargée du contrôle et aux gestionnaires de test de l'état d'avancement du TIFM, et le fournisseur de renseignements sur les menaces reste disponible pour consultation et pour des renseignements supplémentaires sur les menaces lorsque l'équipe chargée du contrôle en fait la demande.

8. L'équipe chargée du contrôle fournit en temps utile des coups de pouce conçus sur la base du plan de test de l'équipe rouge. Des coups de pouce peuvent être ajoutés ou adaptés après approbation de l'équipe chargée du contrôle et des gestionnaires de test.

9. En cas de détection des activités de test par un membre du personnel de l'entité financière ou de ses prestataires tiers de services TIC ou de son prestataire de services TIC intra-groupe, le cas échéant, l'équipe chargée du contrôle, en concertation avec les testeurs et sans préjudice du paragraphe 10, propose et soumet, pour validation, aux gestionnaires de test des mesures permettant de poursuivre le TIFM tout en garantissant sa confidentialité.

10. Dans des circonstances exceptionnelles entraînant des risques d'incidence sur les données, de dommages aux actifs et de perturbation des fonctions, services ou opérations critiques ou importants de l'entité financière elle-même, de ses prestataires tiers de services TIC ou de ses prestataires de services TIC intra-groupe, ou de perturbations pour ses contreparties ou le secteur financier, le chef de l'équipe chargée du contrôle peut suspendre le TIFM ou, en dernier recours, si la poursuite du TIFM n'est pas possible autrement et sous réserve de validation préalable par l'autorité TIFM, poursuivre le TIFM dans le cadre d'un exercice restreint de collaboration violette. La durée de cet exercice restreint de collaboration violette est prise en compte dans le calcul de la durée minimale de 12 semaines de la phase active de test de l'équipe rouge visée au paragraphe 5.

Article 12

Phase de clôture

1. À l'issue de la phase active de test de l'équipe rouge, le chef de l'équipe chargée du contrôle informe l'équipe bleue qu'un TIFM a eu lieu.

2. Dans un délai de quatre semaines à compter de la fin de la phase active de test de l'équipe rouge, les testeurs soumettent à l'équipe chargée du contrôle le rapport de test de l'équipe rouge contenant les informations prévues à l'annexe V.

3. L'équipe chargée du contrôle transmet le rapport de test de l'équipe rouge à l'équipe bleue et aux gestionnaires de test sans retard injustifié.

À la demande des gestionnaires de test, le rapport visé au premier alinéa ne contient pas d'informations sensibles.

4. À la réception du rapport de test de l'équipe rouge, et au plus tard dix semaines après la fin de la phase active de test de l'équipe rouge, l'équipe bleue soumet à l'équipe chargée du contrôle un rapport de test de l'équipe bleue contenant les informations prévues à l'annexe VI. L'équipe chargée du contrôle communique le rapport de test de l'équipe bleue aux testeurs et aux gestionnaires de test sans retard injustifié.

À la demande des gestionnaires de test, le rapport visé au premier alinéa ne contient pas d'informations sensibles.

5. Au plus tard dix semaines après la fin de la phase active de test de l'équipe rouge, l'équipe bleue et les testeurs rejouent les actions offensives et défensives menées pendant le TIFM. L'équipe chargée du contrôle mène également un exercice de collaboration violette sur des sujets déterminés conjointement par l'équipe bleue et les testeurs, sur la base des vulnérabilités recensées lors du test et, le cas échéant, sur des questions qui n'ont pas pu être testées au cours de la phase active de test de l'équipe rouge.

6. À l'issue des exercices de «rejeu» et de collaboration violette, l'équipe chargée du contrôle, l'équipe bleue, les testeurs et les fournisseurs de renseignements sur les menaces se fournissent mutuellement un retour d'information sur le processus de TIFM. Les gestionnaires de test peuvent également fournir un retour d'information.

7. Une fois que l'autorité TIFM a notifié au chef de l'équipe chargée du contrôle qu'elle estime que les rapports de test des équipes bleue et rouge contiennent les informations prévues aux annexes V et VI, l'entité financière soumet pour approbation à l'autorité TIFM, dans un délai de huit semaines, le rapport de synthèse résumant les conclusions pertinentes du TIFM et contenant les éléments prévus à l'annexe VII, conformément à l'article 26, paragraphe 6, du règlement (UE) 2022/2554.

À la demande de l'autorité TIFM, le rapport visé au premier alinéa ne contient pas d'informations sensibles.

Article 13

Plan de mesures correctives

1. Dans un délai de huit semaines à compter de la notification visée à l'article 12, paragraphe 7, du présent règlement, l'entité financière fournit les plans de mesures correctives et la documentation visés à l'article 26, paragraphe 6, du règlement (UE) 2022/2554 à l'autorité TIFM et, si ce n'est pas la même autorité, à l'autorité compétente de l'entité financière.

2. Le plan de mesures correctives visé au paragraphe 1 comprend, pour chaque constatation faite dans le cadre du TIFM:

a) une description des lacunes constatées;

b) une description des mesures correctives proposées, indiquant leur hiérarchisation et la date prévue de réalisation, y compris, le cas échéant, des mesures visant à améliorer les capacités d'identification, de protection, de détection et de réponse;

c) une analyse des causes originelles;

d) le personnel ou les fonctions de l'entité financière chargés de la mise en œuvre des mesures correctives ou des améliorations proposées;

e) les risques associés à la non-mise en œuvre des mesures visées au point b) et, le cas échéant, les risques associés à la mise en œuvre de ces mesures.

Article 14

Attestation

1. L'attestation visée à l'article 26, paragraphe 7, du règlement (UE) 2022/2554 contient les informations prévues à l'annexe VIII.

2. Lorsque plusieurs autorités TIFM ont participé à un TIFM, l'autorité TIFM chef de file fournit l'attestation visée à l'article 26, paragraphe 7, du règlement (UE) 2022/2554 aux entités financières testées.

Article 15

Recours à des testeurs internes

1. Les entités financières mettent en place l'ensemble des modalités suivantes en ce qui concerne le recours à des testeurs internes:

a) l'établissement et la mise en œuvre d'une politique de gestion des testeurs internes dans le cadre d'un TIFM;

b) des mesures visant à garantir que le recours à des testeurs internes pour effectuer un TIFM n'a pas d'incidence négative sur les capacités générales de défense ou de résilience de l'entité financière en ce qui concerne les incidents liés aux TIC ni d'incidence significative sur la disponibilité des ressources consacrées aux tâches liées aux TIC durant un TIFM;

c) des mesures visant à garantir que les testeurs internes disposent de ressources et de capacités suffisantes pour effectuer un TIFM.

La politique visée au point a):

a) contient des critères permettant d'évaluer l'adéquation, les compétences et les conflits d'intérêts potentiels des testeurs internes et précise les responsabilités de gestion dans le cadre du processus de test;

b) est documentée et réexaminée périodiquement;

c) prévoit que l'équipe de test interne est composée d'un chef et d'au moins deux autres membres;

d) exige que tous les membres de l'équipe de test aient fait partie des salariés de l'entité financière ou d'un prestataire de services TIC intra-groupe pendant les 12 derniers mois;

e) prévoit des dispositions concernant la formation des testeurs internes à la réalisation de tests d'intrusion et de tests en équipe rouge.

2. Lorsqu'une autorité TIFM approuve le recours à des testeurs internes conformément à l'article 27, paragraphe 2, point a), du règlement (UE) 2022/2554, elle prend en considération les exigences énoncées à l'article 7, paragraphe 1, du présent règlement.

3. Lorsqu'elle a recours à des testeurs internes, l'entité financière veille à ce que cela soit mentionné dans les documents suivants:

a) les informations concernant le lancement du test visées à l'article 9;

b) le rapport de test de l'équipe rouge visé à l'article 12, paragraphe 2;

c) le rapport de synthèse résumant les conclusions pertinentes du TIFM visé à l'article 26, paragraphe 6, du règlement (UE) 2022/2554.

4. Les testeurs salariés d'un prestataire de services TIC intra-groupe sont considérés comme des testeurs internes de l'entité financière.

Article 16

Coopération et reconnaissance mutuelle

1. Aux fins de l'exécution d'un TIFM concernant une entité financière qui fournit des services dans plus d'un État membre, y compris par l'intermédiaire d'une succursale, l'autorité TIFM de ladite entité:

a) détermine quelles autorités TIFM des États membres d'accueil doivent être impliquées, en tenant compte du fait qu'une ou plusieurs fonctions critiques ou importantes sont ou non exploitées dans les États membres d'accueil ou partagées à travers les États membres d'accueil;

b) informe les autorités TIFM identifiées conformément au point a) de la décision de procéder à un TIFM sur l'entité financière;

c) sauf accord contraire des autorités TIFM, l'autorité TIFM de l'entité financière dirige le TIFM.

Les autorités TIFM des États membres d'accueil peuvent, dans un délai de 20 jours ouvrables à compter de la réception des informations relatives à la conduite future d'un TIFM, soit faire part de leur intérêt à suivre le TIFM en qualité d'observatrices, soit affecter un gestionnaire de test à ce TIFM. L'autorité TIFM chef de file fournit à toutes les autorités TIFM agissant en qualité d'observatrices dans le cadre du TIFM le document de spécification du périmètre du test, le rapport de synthèse du test, le plan de mesures correctives et l'attestation.

L'autorité TIFM chef de file coordonne toutes les autorités TIFM participantes tout au long du test et adopte toutes les décisions nécessaires pour exécuter le TIFM de manière appropriée et efficace. L'autorité TIFM chef de file peut fixer un nombre maximal d'autorités TIFM participantes, dans l'hypothèse où le bon déroulement du TIFM risquerait être compromis en l'absence d'une telle mesure.

2. Lorsqu'une entité financière recourt au même prestataire de services TIC intra-groupe que d'autres entités financières établies dans d'autres États membres, ou appartient à un groupe et partage des systèmes de TIC avec d'autres entités financières du même groupe établies dans d'autres États membres, l'autorité TIFM de l'entité financière prend contact avec les autorités TIFM de ces autres entités financières et évalue avec elles la faisabilité et l'opportunité d'un TIFM commun en ce qui les concerne. Il convient de donner la préférence à un TIFM commun plutôt qu'à un TIFM individuel s'il peut permettre de réduire les coûts et les ressources à la charge des entités financières et des autorités TIFM, pour autant que l'intégrité et l'efficacité du test n'en pâtissent pas.

3. Aux fins de la réalisation d'un TIFM commun:

a) les autorités TIFM des entités financières conviennent de l'entité financière qui sera désignée pour réaliser le TIFM, en prenant en considération la structure du groupe et l'efficacité du test;

b) l'autorité TIFM de l'entité financière désignée conformément au point a) dirige le TIFM, sauf accord contraire des autorités TIFM des entités financières participant au TIFM commun;

c) les autorités TIFM des entités financières autres que l'entité financière désignée pour diriger le TIFM commun peuvent soit faire part de leur intérêt à suivre le TIFM en qualité d'observatrices, soit affecter un gestionnaire de test à ce TIFM.

L'autorité TIFM chef de file coordonne toutes les autorités TIFM impliquées dans le TIFM commun et adopte toutes les décisions nécessaires pour exécuter le TIFM commun de manière rationnelle et efficace.

4. Lorsqu'une entité financière entend réaliser un TIFM groupé, au sens de l'article 26, paragraphe 4, du règlement (UE) 2022/2554, qui pourrait impliquer des entités financières établies dans d'autres États membres, son autorité TIFM prend contact avec les autorités TIFM de ces autres entités financières et évalue avec elles la faisabilité et l'opportunité d'un TIFM groupé en ce qui les concerne conformément à l'article 26, paragraphe 4, du règlement (UE) 2022/2554.

5. Aux fins de la conduite d'un TIFM groupé au sens de l'article 26, paragraphe 4, du règlement (UE) 2022/2554:

a) les autorités TIFM des entités financières conviennent de l'entité financière qui sera désignée pour conduire le TIFM groupé, en prenant en considération les services TIC fournis par le prestataire tiers de services TIC aux entités financières et l'efficacité du test;

b) l'autorité TIFM de l'entité financière désignée conformément au point a) dirige le TIFM, sauf accord contraire des autorités TIFM des entités financières participant au TIFM groupé;

c) les autorités TIFM des entités financières autres que l'entité financière désignée pour diriger le TIFM groupé peuvent soit faire part de leur intérêt à suivre le test en qualité d'observatrices, soit affecter un gestionnaire de test à ce TIFM.

L'autorité TIFM chef de file coordonne toutes les autorités TIFM impliquées dans le TIFM groupé et adopte toutes les décisions nécessaires pour exécuter le TIFM groupé de manière rationnelle et efficace.

6. S'agissant d'une entité financière tenue d'effectuer un TIFM, lorsque son autorité TIFM est différente de son autorité compétente au sens de l'article 46 du règlement (UE) 2022/2554, ces autorités partagent toute information pertinente concernant l'ensemble des questions liées aux TIFM aux fins de l'exécution des tests ou de l'accomplissement de leurs tâches conformément audit règlement.

Article 17

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 13 février 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Contenu de la charte de projet [article 9, paragraphe 2, point a)]

Élément d'information	Informations requises
Personne responsable du plan du projet, à savoir le chef de l'équipe chargée du contrôle	Nom Coordonnées
Testeurs	☐ internes ☐ externes ☐ les deux
Canaux de communication sélectionnés conformément à l'article 9, paragraphe 2, point d), et à l'article 9, paragraphe 4, point a), y compris: a) le système de cryptage à utiliser pour le courrier électronique b) les salles de données en ligne (data room) à utiliser c) la messagerie instantanée à utiliser	
Nom de code du TIFM	
Le cas échéant, les fonctions critiques ou importantes que l'entité financière exerce dans d'autres États membres	1. La liste des fonctions critiques ou importantes exercées dans un autre État membre 2. Pour chaque fonction critique ou importante, l'indication du ou des États membres dans lesquels elles sont exercées
Le cas échéant, les fonctions critiques ou importantes soutenues par des prestataires tiers de services TIC	3. La liste des fonctions critiques ou importantes soutenues par des prestataires tiers de services TIC, le cas échéant 4. Pour chaque fonction, l'identification du prestataire tiers de services TIC
Dates limites prévues pour l'achèvement de:	
1) la phase de préparation, conformément à l'article 9	aaaa-mm-jj
2) la phase de test, conformément aux articles 10 et 11	aaaa-mm-jj
3) la phase de clôture, conformément à l'article 12	aaaa-mm-jj
4) du plan de mesures correctives, conformément à l'article 13	aaaa-mm-jj

ANNEXE II

Préparation du document de spécification du périmètre du test (article 9, paragraphe 6)

1. Le document de spécification du périmètre du test doit contenir une liste de toutes les fonctions critiques ou importantes identifiées par l'entité financière.

2. Les informations suivantes doivent être incluses pour chaque fonction critique ou importante identifiée:

   a) si la fonction critique ou importante n'est pas incluse dans le périmètre du TIFM, l'explication des raisons de cette non-inclusion;

   b) si la fonction critique ou importante est incluse dans le périmètre du TIFM:

      i) l'explication des raisons de son inclusion;

      ii) le ou les systèmes de TIC identifiés qui soutiennent cette fonction critique ou importante;

      iii) pour chaque système de TIC identifié:

         1. s'il est externalisé et, dans l'affirmative, le nom du prestataire tiers de services TIC,

         2. les pays et territoires dans lesquels le système de TIC est utilisé,

         3. une description de haut niveau du ou des drapeaux préliminaires, indiquant quel aspect de sécurité touchant à la confidentialité, à l'intégrité, à l'authenticité ou à la disponibilité est couvert par chaque drapeau.

ANNEXE III

Contenu du rapport de renseignement sur les menaces ciblées (article 10, paragraphe 5)

Le rapport de renseignement sur les menaces ciblées contient des informations sur tous les points suivants:

1. Le périmètre global de la recherche en matière de renseignement, dont au moins les éléments suivants:
   a) les fonctions critiques ou importantes entrant dans le périmètre;
   b) leur localisation géographique;
   c) la langue officielle de l'UE utilisée;
   d) les prestataires tiers de services TIC concernés;
   e) la période au cours de laquelle les renseignements sont recueillis.
2. Une évaluation globale indiquant quels renseignements concrets exploitables peuvent être trouvés au sujet de l'entité financière, notamment:
   a) les noms d'utilisateur et les mots de passe des salariés;
   b) les domaines ressemblants susceptibles d'être confondus avec les domaines officiels de l'entité financière;
   c) la reconnaissance technique: logiciels, systèmes et technologies vulnérables ou exploitables;
   d) les informations publiées par les salariés sur l'internet concernant l'entité financière, qui pourraient être utilisées aux fins d'une attaque;
   e) les informations en vente sur le dark web;
   f) toute autre information pertinente disponible sur l'internet ou sur les réseaux publics;
   g) le cas échéant, des informations de ciblage physique, y compris les modalités d'accès aux locaux de l'entité financière.
3. L'analyse des renseignements sur les menaces à la lumière du panorama général de la menace et de la situation particulière de l'entité financière, y compris, au moins:
   a) l'environnement géopolitique;
   b) l'environnement économique;
   c) les évolutions technologiques et toute autre évolution concernant les activités dans le secteur des services financiers.
4. Les profils de menace des acteurs malveillants (personne/groupe spécifique ou catégorie générique) susceptibles de cibler l'entité financière, y compris les systèmes de l'entité financière que les acteurs malveillants sont les plus susceptibles de compromettre ou de cibler, la motivation, l'intention et la logique possibles du ciblage potentiel et le mode opératoire possible des auteurs des attaques.
5. Les scénarios de menace: au moins trois scénarios de menace de bout en bout pour les profils de menace identifiés conformément au point 4 qui présentent les scores de gravité de la menace les plus élevés. Les scénarios de menace décrivent le chemin d'attaque de bout en bout et comprennent au moins:
   a) un scénario qui inclut, sans s'y limiter, la compromission de la disponibilité du service;
   b) un scénario qui inclut, sans s'y limiter, la compromission de l'intégrité des données;
   c) un scénario qui inclut, sans s'y limiter, la compromission de la confidentialité des informations.
6. Le cas échéant, une description du scénario non fondé sur la menace visé à l'article 10, paragraphe 4.

ANNEXE IV

Contenu du plan de test de l'équipe rouge (article 11, paragraphe 1)

Le plan de test de l'équipe rouge doit contenir des informations sur tous les éléments suivants:

a) les canaux et procédures de communication;

b) les tactiques, techniques et procédures autorisées ou non autorisées lors de l'attaque, y compris les limites éthiques de l'ingénierie sociale;

c) les mesures de gestion des risques à suivre par les testeurs;

d) une description de chaque scénario, comprenant:

   i) l'acteur de la menace simulée;

   ii) son intention, sa motivation et ses objectifs;

   iii) la (les) fonction(s) cible(s) et le(s) système(s) de TIC qui la (les) soutiennent;

   iv) les aspects ciblés de confidentialité, d'intégrité, de disponibilité et d'authenticité;

   v) les drapeaux.

e) une description détaillée de chaque chemin d'attaque prévu, en ce compris les prérequis et les éventuels coups de pouce à fournir par l'équipe chargée du contrôle, ainsi que les délais pour leur fourniture et leur utilisation potentielle;

f) la programmation des activités de l'équipe rouge, y compris la planification chronologique de l'exécution de chaque scénario, décomposée au moins selon les trois phases qu'un testeur suit au cours de la phase de test, à savoir s'introduire dans les systèmes de TIC des entités financières, se déplacer dans les systèmes de TIC pour, au final exécuter des actions sur les objectifs puis, en bout de course, s'extraire des systèmes de TIC (phases d'entrée, de circulation et de sortie);

g) les particularités de l'infrastructure des entités financières à prendre en considération lors des tests;

h) le cas échéant, des informations complémentaires ou d'autres ressources nécessaires aux testeurs pour exécuter les scénarios.

ANNEXE V

Contenu du rapport de test de l'équipe rouge (article 12, paragraphe 2)

Le rapport de test de l'équipe rouge doit contenir des informations sur au moins tous les points suivants:

a) des informations sur l'attaque menée, y compris:

   i) les fonctions critiques ou importantes ciblées et les systèmes, processus et technologies de TIC identifiés qui soutiennent les fonctions critiques ou importantes en question, tels qu'identifiés dans le plan de test de l'équipe rouge;

   ii) le résumé de chaque scénario;

   iii) les drapeaux atteints et non atteints;

   iv) les chemins d'attaque suivis avec succès et sans succès;

   v) les tactiques, techniques et procédures utilisées avec succès et sans succès;

   vi) les écarts par rapport au plan de test de l'équipe rouge, le cas échéant;

   vii) les coups de pouce fournis, le cas échéant;

b) toutes les actions dont les testeurs ont connaissance et qui ont été réalisées par l'équipe bleue pour reconstruire l'attaque et en atténuer les effets;

c) les vulnérabilités découvertes et autres constatations, y compris:

   i) une description de la vulnérabilité et des autres constatations, dont leur criticité;

   ii) une analyse des causes originelles de la réussite des attaques menées à bien;

   iii) des recommandations en matière de mesures correctives, avec indication de leur degré de priorité.

ANNEXE VI

Contenu du rapport de test de l'équipe bleue (article 12, paragraphe 4)

Le rapport de test de l'équipe bleue contient des informations sur au moins tous les points suivants:

1. Pour chaque étape de l'attaque décrite par les testeurs dans le rapport de test de l'équipe rouge:
   a) une liste des actions offensives détectées;
   b) les entrées de journal (log entries) correspondant à ces détections.
2. L'évaluation des constatations et recommandations des testeurs.
3. Les preuves de l'attaque par les testeurs recueillies par l'équipe bleue.
4. L'analyse par l'équipe bleue des causes originelles de la réussite des attaques menées à bien par les testeurs.
5. La liste des enseignements tirés et les possibilités d'amélioration identifiées.
6. La liste des sujets à traiter dans le cadre de la collaboration violette.

ANNEXE VII

Détails du rapport de synthèse résumant les conclusions pertinentes du TIFM visé à l'article 26, paragraphe 6, du règlement (UE) 2022/2554

Le rapport de synthèse du test contient des informations sur au moins tous les points suivants:

a) les parties concernées;

b) le plan du projet;

c) le périmètre validé, y compris la justification de l'inclusion ou de l'exclusion de fonctions critiques ou importantes et de systèmes, processus et technologies de TIC identifiés qui soutiennent les fonctions critiques ou importantes couvertes par le TIFM;

d) les scénarios sélectionnés et tout écart important par rapport au rapport de renseignement sur les menaces ciblées;

e) les chemins d'attaque exécutés et les tactiques, techniques et procédures utilisées;

f) les drapeaux atteints et non atteints;

g) les écarts par rapport au plan de test de l'équipe rouge, le cas échéant;

h) les détections de l'équipe bleue, le cas échéant;

i) la collaboration violette pendant la phase de test, le cas échéant, et les conditions associées;

j) les coups de pouce utilisés, le cas échéant;

k) les mesures de gestion des risques adoptées;

l) les vulnérabilités identifiées et autres constatations, avec mention de leur criticité;

m) une analyse des causes originelles de la réussite des attaques menées à bien;

n) un plan de haut niveau pour les mesures correctives, établissant un lien entre les vulnérabilités et les autres constatations, leurs causes originelles et leur priorité en matière de mesures correctives;

o) les enseignements tirés des retours d'information reçus.

ANNEXE VIII

Détails de l'attestation de TIFM visée à l'article 26, paragraphe 7, du règlement (UE) 2022/2554

L'attestation contient au moins toutes les informations suivantes:

a) concernant le TIFM réalisé:

   i) les dates de début et de fin du TIFM;

   ii) les fonctions critiques ou importantes incluses dans le périmètre du test;

   iii) le cas échéant, des informations sur les fonctions critiques ou importantes incluses dans le périmètre du test pour lesquelles le TIFM n'a pas été exécuté;

   iv) le cas échéant, les autres entités financières impliquées dans le TIFM;

   v) le cas échéant, les prestataires tiers de services TIC qui ont participé au TIFM;

   vi) en ce qui concerne les testeurs:

      1. s'il a été fait appel à des testeurs internes;

      2. si l'entité financière a eu recours à l'article 5, paragraphe 3, deuxième alinéa;

   vii) la durée, en jours calendaires, de la phase active de test de l'équipe rouge;

b) lorsque plusieurs autorités TIFM ont été impliquées dans le TIFM, les autres autorités TIFM qui ont été impliquées, et en quelle qualité;

c) la liste des documents examinés par l'autorité TIFM aux fins de l'attestation.