GROUPE DES SEPT – ÉLÉMENTS FONDAMENTAUX POUR L'ÉVALUATION EFFICACE DE LA CYBERSÉCURITÉ DANS LE SECTEUR FINANCIER

Résumé
Considérant la propagation des cyber-risques et la nécessité d'efforts soutenus pour améliorer la cybersécurité dans le secteur financier, le G7 a élaboré un ensemble d'éléments fondamentaux pour évaluer efficacement la cybersécurité.

Le G7 a publié en octobre 2016 le document appelé *Groupe des sept – Éléments fondamentaux pour la cybersécurité du secteur financier* (« *G7EF* »). Ce document a présenté un ensemble de pratiques efficaces de cybersécurité pour les entités privées, les autorités publiques, et le secteur financier (« les entités »). Son objectif est d'accroître la résilience du système financier en aidant les entités privées et publiques à concevoir et mettre en œuvre des politiques de cybersécurité et des mesures opérationnelles. Les *G7EF* sont formulés comme des principes généraux et non contraignants, qui forment un socle sur lequel une entité (privée ou publique) peut concevoir et mettre en œuvre son approche en matière de cybersécurité, dans le cadre de sa gestion et sa culture du risque.

Les *G7 – Éléments fondamentaux pour l'évaluation efficace* soutiennent l'application des pratiques efficaces prévues par les *G7EF* en visant à mesurer si celles-ci sont bien mises en place et évaluées. Les *G7EF* auront ainsi une plus grande incidence s'ils sont assortis d'un ensemble de résultats souhaitables (Partie A), et d'un processus pour leur évaluation et leur examen (Partie B). Plus particulièrement :

- La Partie A décrit cinq **résultats souhaitables** qu'une entité qualifiée pourrait présenter et auxquels des entités moins qualifiées peuvent aspirer. Les résultats s'appuient sur les *G7EF*, en encourageant les entités à continuer d'améliorer leur cybersécurité, et en fournissant d'autres caractéristiques pour évaluer l'efficacité des capacités de cybersécurité (le « quoi »).

- La Partie B établit cinq **éléments d'évaluation** que les évaluateurs peuvent utiliser pour élaborer leur méthode d'évaluation des progrès à mesure que les entités élaborent et améliorent leur cadre de cybersécurité. Les éléments visent à promouvoir la qualité des évaluations de cybersécurité afin de faciliter un processus d'amélioration continue. Ils renseignent également sur la qualité de l'appréciation du champ de l'évaluation, ainsi que sur l'exécution, et la communication des résultats de l'évaluation. Ensemble, ils facilitent l'évaluation en décrivant l'efficacité des évaluations de cybersécurité (le « comment »).

Résultats souhaitables	Éléments d'évaluation
1. Les Éléments fondamentaux (G7EF) sont mis en œuvre. 2. L'organisation de la prise de décision tient compte de la cybersécurité. 3. Il est admis qu'une perturbation se produira. 4. Une approche adaptative de cybersécurité est adoptée. 5. Il existe une culture qui favorise des comportements sécuritaires.	1. Établir des objectifs clairs d'évaluation. 2. Établir et communiquer la méthodologie et les attentes. 3. Maintenir une palette diversifiée d'outils d'évaluation et un processus de sélection de ces outils. 4. Rendre compte de manière claire des conclusions et formuler des mesures correctives concrètes. 5. S'assurer que les évaluations sont fiables et justes.

Les G7 – Éléments fondamentaux pour l'évaluation efficace constituent des outils pour orienter et mener des discussions internes et externes sur les décisions en matière de gestion des risques qui sont essentielles à la cybersécurité. Par exemple, ils peuvent aider à éclairer le conseil d'administration dans ses discussions et ses actions de surveillance. Les *G7 – Éléments fondamentaux pour l'évaluation efficace* n'ont pas de caractère prescriptif, et permettent d'informer les entités, les superviseurs et les évaluateurs indépendants. Ils peuvent également servir dans les vérifications menées par les régulateurs, les auto-évaluations, et l'examen indépendant effectué par des tiers. De plus, ces éléments peuvent faciliter les échanges de nature technique et culturelle entre plusieurs juridictions et secteurs sur les pratiques efficaces de gestion des cyber-risques.

PARTIE A : Résultats liés à une cybersécurité efficace

Tout en admettant qu'il existe de multiples façons de décrire la cybersécurité, les cinq résultats souhaitables ci-dessous établissent des caractéristiques générales qu'une entité du secteur financier ayant un niveau avancé de compréhension, de réalisation et de surveillance de sa cybersécurité peut présenter à un évaluateur.

Résultat 1 : Les *Éléments fondamentaux* (G7EF) sont mis en œuvre.
Les *G7EF* offrent les blocs constitutifs de cybersécurité à la fois aux entités qui en sont aux premiers stades pour bâtir leur cyber-résilience et à celles qui sont plus avancées.

Les *G7EF* ont une portée générale, reflétant la nature du défi. Une cybersécurité efficace exige que les entités tiennent à jour une stratégie et un cadre de cybersécurité (*Élément 1*) et qu'elles adaptent ou renforcent leurs processus de gouvernance (*Élément 2*). Elle exige la mise en place de cadres de gestion et de maîtrise des risques, y compris un ensemble approprié de contrôles d'atténuation et de mécanismes de protection (*Élément 3*) et une surveillance efficace (*Élément 4*). Des procédures d'intervention (Élément 5) et de reprise (Élément 6) clairement définies et examinées régulièrement sont en place en cas de cyber-incidents. Enfin, l'échange de renseignements (*Élément* 7) et l'apprentissage continu (*Élément 8*) renforcent les *G7EF* et permettent de consolider la cybersécurité globale.

Résultat 2 : L'organisation de la prise de décision tient compte de la cybersécurité.
En s'appuyant sur l'*Élément 1* (Stratégie et cadre de cybersécurité) et l'*Élément 2* (Gouvernance), l'intégration de la cybersécurité dans les processus normaux de prise de décision, plus particulièrement en intégrant la gestion des cyber-risques tôt dans ces processus, éclaire et facilite les résultats stratégiques dans toute l'organisation. La cybersécurité ne doit pas être vue distinctement de la conception et du fonctionnement des processus opérationnels des entités, mais plutôt comme un élément stratégique essentiel, tant au moment d'élaborer de nouveaux produits et services qu'au moment d'évaluer l'efficacité des activités opérationnelles qui utilisent la technologie ou les infrastructures existantes.

L'engagement actif des dirigeants ou du conseil d'administration suppose la surveillance de la conception, de la mise en œuvre et de l'efficacité des programmes de cybersécurité. Éclairés par les renseignements sur les menaces et les vulnérabilités et l'appétit au risque de leur entité, le conseil d'administration et les dirigeants peuvent orienter sur le court terme et le long terme les décisions de gestion des risques, les actions de surveillance et les principes de responsabilité. Par conséquent,

le conseil d'administration et les dirigeants peuvent utiliser la prise de décision pour orienter des programmes de cybersécurité au-delà d'une vision traditionnelle de la conformité.

Résultat 3 : Il est admis qu'une perturbation se produira.
En se fondant sur l'*Élément 3* (évaluation des risques et des contrôles), la superposition des contrôles de détection et de protection est essentielle, et réduit la probabilité d'une perte de disponibilité, d'intégrité ou de confidentialité. Toutefois, les entités avancées reconnaissent qu'il est impossible de garantir un environnement à l'épreuve de toute défaillance. En admettant que des perturbations opérationnelles se produiront, les principaux décideurs comprennent que les décisions d'investissements conformes à la stratégie doivent couvrir de manière équilibrée tous les aspects des *G7EF*.

Les entités qui ne reconnaissent pas ce concept peuvent présenter un déséquilibre en ayant une grande dépendance sur les contrôles périmétriques, au détriment d'une capacité d'intervention clairement définie et testée régulièrement (*Élément 5*) et d'un plan de rétablissement fiable et testé pour la reprise des activités (*Élément 6*).

Résultat 4 : Une approche adaptative de cybersécurité est adoptée.
De nouvelles vulnérabilités et cyber-menaces les exploitant apparaissent et évoluent en permanence. En conséquence, les entités doivent faire preuve de capacité d'adaptation et ne pas adopter une approche de défense statique pour s'assurer que leurs procédures de cybersécurité tiennent compte de l'environnement évolutif dans lequel elles travaillent.

En se fondant sur l'*Élément 5* (intervention) et l'*Élément 6* (reprise), les mécanismes d'intervention en cas d'incident doivent être bien exécutés afin que les fonctions économiques puissent continuer à opérer en cas d'interruption ou de crise, que ce soit au niveau de l'entité, du secteur, de plusieurs secteurs ou au niveau international. Puisque les interruptions peuvent toucher le secteur financier de manières imprévues, la souplesse est essentielle dans les fonctions réactives. Conjuguées à l'*Élément 4* (surveillance), l'agilité et l'expérience avec laquelle une entité peut détecter et maîtriser rapidement des interruptions influent beaucoup sur les répercussions. Par conséquent, l'objectif global doit être de favoriser un environnement d'amélioration et d'apprentissage continus dans le cadre du programme de cybersécurité.

Résultat 5 : Il existe une culture qui favorise des comportements sécuritaires.
En se fondant sur l'*Élément 7* (échange de renseignements) et l'*Élément 8* (apprentissage continu), il est essentiel de mettre en permanence l'accent sur les compétences et les comportements pour intégrer une cybersécurité efficace dans la structure d'une organisation.

Pour beaucoup d'incidents de cybersécurité, ce sont des procédures défectueuses ou des facteurs humains qui sont en cause (par exemple, l'exploitation des mots de passe faibles, l'ingénierie sociale, la faible sensibilisation à la sécurité, etc.). Des stratégies de mise en œuvre d'une cybersécurité efficace tiennent tout autant compte des éléments reliés aux personnes et aux processus que des solutions techniques, y compris dans les décisions d'investissements. La formation et la sensibilisation de l'utilisateur final, de l'employé et des dirigeants sont tout aussi importantes.

À une époque où la facilité d'usage l'emporte souvent sur la sécurité, la manipulation de la psychologie humaine par un adversaire peut être aussi redoutable que sa maîtrise technologique. Chaque personne comprend qu'elle a un rôle à jouer. La cybersécurité efficace suppose de

mobiliser et former les personnes, et leur permettre de gérer l'information en toute sécurité. La formation et la sensibilisation à la cybersécurité peuvent améliorer les connaissances techniques, et offrir des occasions pour changer les comportements. La formation efficace vise un changement réel et mesurable, en façonnant la culture de façon significative, au lieu de rechercher la conformité à un ensemble de politiques. L'adage qui dit que les personnes sont considérées comme le maillon le plus faible est inversé, et on les considère plutôt comme la ressource la plus précieuse.

PARTIE B : Promouvoir des évaluations efficaces de cybersécurité

À mesure que les entités intègrent les *G7FE* et s'efforcent d'atteindre les résultats souhaitables décrits ci-dessus, il est nécessaire d'effectuer des évaluations régulières pour mesurer l'efficacité de leurs programmes de cybersécurité.

On peut définir l'évaluation de la cybersécurité comme la collecte, l'examen et l'utilisation systématiques des renseignements sur les pratiques et les contrôles de cybersécurité des entités du secteur financier (privées ou publiques) prises isolément ou des participants du secteur pris collectivement afin de (i) juger le rendement au regard des résultats attendus, et de (ii) indiquer les conclusions et identifier les points d'amélioration ainsi que les mesures correctives.

Pour atteindre ces objectifs, les *G-7 – Éléments fondamentaux pour l'évaluation efficace* ont établi cinq éléments généraux que les entités du secteur financier devraient prendre en compte et intégrer dans leurs cadres d'évaluation de la cybersécurité et leurs évaluations.

Élément 1 : Établir des objectifs clairs d'évaluation.
Les évaluateurs établissent des objectifs d'évaluation précis afin de clarifier l'exercice pour eux-mêmes mais aussi pour l'entité évaluée, et de faciliter l'imputabilité des résultats. Des objectifs clairement définis favorisent également l'amélioration et l'apprentissage en continu.

Les objectifs d'évaluation confirment le champ de l'évaluation, allant d'une évaluation concentrée sur une seule entité (en partie ou intégralement) à un secteur complet. La portée de l'évaluation définit également quels aspects de la cybersécurité sont examinés. Par exemple, les évaluateurs peuvent choisir d'évaluer la performance au regard de toutes sortes de pratiques efficaces, comme les *G7EF* ou d'autres plus détaillées.

Différents critères sont pris en compte pour fixer le champ de l'évaluation, en combinant les aspects qualitatifs et quantitatifs et en veillant à laisser le moins possible des sujets non couverts. La détermination du champ de l'évaluation établit également le périmètre de l'évaluation, en indiquant si tel ou tel lien de dépendance que l'entité a avec d'autres entités ou avec ses fournisseurs sont inclus ou exclus.

Au moment d'établir les objectifs de l'évaluation, les évaluateurs envisagent les différentes approches d'évaluation possibles pour s'assurer que les évaluations sont efficaces et efficientes. De plus, ils tiennent compte des différences de régimes légaux et réglementaires lorsque l'évaluation s'étend à plusieurs juridictions. Dans le cas d'entités complexes, comme des groupes transfrontaliers, plusieurs évaluateurs peuvent s'intéresser aux résultats de l'évaluation. Les évaluateurs ayant des intérêts et des mandats communs sont encouragés à se mettre en relation pour identifier les interdépendances importantes, définir clairement les responsabilités à l'avance, et éviter de formuler des exigences conflictuelles.

Élément 2 : Établir et communiquer la méthodologie et les attentes.
En tenant compte des lignes directrices et des cadres de cybersécurité actuels, les évaluateurs établissent des attentes claires et mesurables au regard desquelles les évaluations de cybersécurité doivent être effectuées. Ces attentes sont communiquées aux entités, et comprises par celles-ci, avant le début de l'évaluation.

La méthodologie choisie par les évaluateurs est cohérente avec les objectifs établis et la complexité de l'entité évaluée. Pour réaliser une évaluation proportionnée, il est possible de suivre une approche basée sur les risques, tout en tenant compte de la nature complexe et dynamique du cyber-risque.

Élément 3 : Maintenir une palette diversifiée d'outils d'évaluation et un processus pour la sélection de ces outils.
Étant donné la nature complexe et variée du cyber-risque, une palette diversifiée d'outils et de techniques d'évaluation (« boîte à outils ») permet de réaliser des évaluations de cybersécurité efficaces. Une telle palette diversifiée contient des méthodes d'évaluation qui tiennent compte de l'étendue, de la couverture, ou de la maturité recherchée dans une évaluation donnée. Elle offre également aux évaluateurs plusieurs approches possibles pour correspondre à une grande variété de situations.

Les boîtes à outils pour l'évaluation de la cybersécurité peuvent comprendre, sans toutefois s'y limiter, des analyses documentaires, des auto-évaluations, des inspections sur place, des tests d'intrusion fondés sur les menaces, des examens techniques (« analyse approfondie »), des examens thématiques, et des exercices. Chaque outil peut donner une assurance sur diverses pratiques et aura ses propres avantages et inconvénients. L'utilisation conjointe de plusieurs outils et techniques réduit le risque de dépendance excessive sur une seule méthode d'évaluation.

Pour faciliter la mise en correspondance de l'outil ou de la technique d'évaluation par rapport aux objectifs définis, un processus de sélection d'outils est recommandé. Au minimum, ce processus de sélection tient compte de l'importance des entités au sein de leur secteur et de leur risque inhérent, de la nature et la portée précises de l'évaluation, des ressources et du temps nécessaires à l'évaluation, ainsi que du niveau d'assurance recherché. Pour évaluer l'efficacité des pratiques de cybersécurité, on recommande aux évaluateurs de sélectionner des outils qui démontrent activement les capacités de l'entité, afin de dépasser le simple examen de ses politiques et procédures.

Les outils d'évaluation sont régulièrement évalués pour s'assurer qu'ils répondent toujours aux objectifs. Le caractère adapté de chaque outil est régulièrement vérifié pour tenir compte de l'évolution des menaces et des activités, ainsi que des ressources disponibles.

Élément 4 : Rendre compte de manière claire des conclusions et formuler des mesures correctives concrètes.
Les évaluations efficaces de cybersécurité fournissent des résultats pertinents pour orienter les décisions et les actions. Cela signifie qu'il faut élaborer des conclusions claires et identifier des mesures correctives concrètes et/ou des constatations thématiques qui peuvent ensuite mener à une action.

Au moment de formuler une conclusion importante, les évaluateurs résument les pratiques observées et les réalisations, et déterminent les écarts et les manquements par rapport aux attentes à

mesure qu'ils apparaissent, à la lumière des faits recueillis. Les évaluateurs décrivent les risques ou autres enjeux connexes et leurs implications. En général, le résultat des évaluations apporte de la valeur, appuie la prise de décision, et produit un compte rendu qui mène à une amélioration importante et durable.

Élément 5 : S'assurer que les évaluations sont fiables et justes.
Des méthodologies d'évaluation robustes peuvent garantir la parité entre les jugements de divers évaluateurs, et l'uniformité globale de l'approche. De plus, la proportionnalité permet de s'assurer que les évaluations effectuées sont pratiques et réalistes.

Les évaluations sont exécutées par des personnes compétentes ayant des niveaux définis de compétences et de connaissances. Étant donné la nature complexe et diversifiée du cyber-risque, une formation solide en informatique ou en cybersécurité est souhaitable, combinée à une compréhension approfondie de l'activité ou du secteur en question. Il peut être utile de faire appel à des évaluateurs qui couvrent individuellement ou collectivement plusieurs disciplines. De plus, pour ne pas être dépassé par les évolutions constantes de l'environnement, il est recommandé que les évaluateurs mettent à jour leurs compétences de façon continue, au moyen de la formation ou d'autres activités professionnelles.

La qualité globale du processus d'évaluation est maintenue au moyen d'examens indépendants (c'est-à-dire, évaluer l'évaluateur) des évaluations effectuées et des méthodologies adoptées, de l'échange de connaissances entre les évaluateurs, et des évaluations d'évaluateur individuel. Pour favoriser l'équité et éviter le parti pris, les entités évaluées bénéficient d'un processus transparent, tout en étant assurées de la confidentialité de la portée, de la méthodologie et des constatations de l'évaluation.