Directives

Évaluation du risque de contrepartie en matière de cybersécurité

Guide de démarrage

Sommaire

Qualifications et conditions limitatives

Le présent document fournit des recommandations générales et non contraignantes aux utilisateurs de SWIFT quant à la manière d'utiliser et d'interpréter les données relatives à la cybersécurité provenant de contreparties de l'écosystème des services financiers. Il propose des suggestions sur l'approche préconisée de gouvernance, et sur les processus de partage et d'intégration des données pour les risques liés à la cybersécurité dans le cadre existant de la gestion des risques d'une institution.

Il ne traite pas des problèmes ou exigences propres à l'utilisateur.

Les informations contenues dans le présent document ne sont pas exhaustives, et ne remplacent pas non plus l'exercice d'un jugement sain ou la conformité aux pratiques exemplaires.

Les utilisateurs sont entièrement et exclusivement responsables des mesures ou décisions prises qui découlent des directives ou recommandations, et de l'interprétation des informations énoncées dans le présent document. SWIFT décline toute responsabilité relative au contenu du présent document, ou relatives aux mesures ou décisions prises sur la base du contenu ou relatives au contenu du présent document ou leurs conséquences. Rien dans le présent document ne doit être interprété ou compris comme constituant une obligation, déclaration ou garantie de la part de SWIFT.

SWIFT fournit le présent document à titre purement informatif. Les informations qui figurent dans le présent document sont susceptibles de changer au fil du temps. Les utilisateurs doivent toujours se référer à la dernière version disponible de ce document.

Voix du client

Quels sont les défis majeurs que vous rencontrez dans le cadre de la gestion du cyber-risque appliquée à vos contreparties ?

« Un défi majeur que nous rencontrons est l'accès aux cyber-contrôles en place chez nos contreparties. Le fait de ne pas connaître le niveau de contrôle chez chaque contrepartie rend la gestion du cyber-risque difficile. Vous êtes seulement aussi fort que votre maillon le plus faible. C'est la raison pour laquelle il est très important d'effectuer des examens de diligence raisonnable sur la cybersécurité des contreparties.

Les problèmes majeurs concernent les activités suivantes :

- Trouver une norme cohérente utilisée par toutes les contreparties qui puisse être exploitée pour définir des indices de référence
- Persuader les contreparties de communiquer des informations sur leurs contrôles ou leur absence de contrôles en matière de sécurité
- Valider l'exactitude des informations fournies par les contreparties
- Utiliser et traiter les données selon des modalités qui procurent à l'entreprise de précieuses informations sur les risques, de manière à ce qu'elle puisse comprendre et prendre des décisions commerciales appropriées
- Suivi des problèmes pour assurer qu'ils sont remédiés et clôturés et pour convenir quant à la mise en œuvre de contrôles compensatoires entre-temps. »

Avant-propos

La cybersécurité demeure une menace majeure pour le secteur des services financiers. Le présent guide indique comment les organisations faisant partie de l'écosystème bancaire et de paiement pourraient aborder l'évaluation du cyber-risque posé par leurs contreparties avec lesquelles elles effectuent des transactions au quotidien.

Les directives couvrent quatre domaines que chaque institution devrait chercher à traiter : définir un modèle de gouvernance ; définir un cadre de gestion des risques cybernétiques ; adopter des contre-mesures sur les risques cybernétiques et intégrer les données d'« attestation » de la cybersécurité provenant des contreparties.

Les risques liés à la cybersécurité, y compris ceux qui proviennent des contreparties, doivent être gérés avec d'autres types de risques : opérationnels, financiers et réglementaires. De nombreuses institutions s'appliquent à intégrer l'évaluation du cyber-risque dans leurs processus existants et relatif au risque de contrepartie.

La supervision de ce processus – la **gouvernance** – doit être organisée de manière à ce que les personnes compétentes qui assument des responsabilités adéquates puissent prendre des décisions, et que les processus soient robustes et répétables. En ayant une structure de gouvernance bien assise, les institutions peuvent aborder la mise en œuvre d'un **cadre de gestion** des risques liés à la cybersécurité. Ce travail englobe l'évaluation du risque de contrepartie en :

- recueillant les données nécessaires pour appuyer les décisions axées sur le risque ;
- traitant ces données et en les transformant en une évaluation pondérée, basée sur les risques, apparaissant généralement sous forme de note numérique ou d'indicateur rouge-orange-vert ;
- adoptant des contre-mesures appropriées pour atténuer ou « traiter » les risques.

Les institutions peuvent avoir des appétits différents en matière de risque mais, à titre d'exemples, les contre-mesures d'atténuation des risques liés à la cybersécurité peuvent consister à :

- appliquer des niveaux de contrôles supplémentaires aux transactions provenant de la contrepartie ;
- limiter le type de transactions conclues avec la contrepartie ;
- demander à la contrepartie de mettre en œuvre d'autres contrôles ou mesures de détection de la fraude ;
- demander à la contrepartie de justifier ses informations par le biais d'une évaluation indépendante ;
- réévaluer les accords et contrats conclus avec la contrepartie.

Dans le cadre de ce modèle de gouvernance et de gestion des risques, les institutions devraient envisager d'intégrer les données sur l'état de préparation de leurs contreparties en matière de cybersécurité.

Le Customer Security Controls Framework (CSCF – Cadre des contrôles de sécurité des clients) que SWIFT a introduit en tant qu'élément de son Customer Security Programme (CSP – Programme relatif à la sécurité des clients) est très précieux à cet égard. Le CSCF décrit un ensemble de contrôles de sécurité obligatoires et recommandés aux utilisateurs SWIFT, établissant une base en matière de sécurité pour toute la collectivité. Tous les utilisateurs doivent le mettre en application dans leur infrastructure SWIFT locale, et ils doivent évaluer eux-mêmes leur conformité aux contrôles de sécurité obligatoires.

Une fois que les auto-évaluations ont été publiées, les utilisateurs peuvent les mettre à la disposition de leurs contreparties, prouvant leur conformité à chaque contrôle individuel, et de la même façon, les contreparties peuvent exiger de les recevoir entre eux. Les utilisateurs peuvent afficher et exporter les données, soit contrepartie par contrepartie, ou en vrac, pour mieux « **utiliser** » les données et les intégrer dans leurs cadres décisionnels de risques.

Le CSCF contribue à accroître la transparence et la normalisation de la communauté pour mieux permettre aux organisations d'intégrer la cybersécurité dans leurs prises de décisions. Ces données d'attestation sont riches en informations et une source unique de données sur les risques liés à la cybersécurité pour les utilisateurs de SWIFT.

Contexte

La cybersécurité et la fraude demeurent des menaces mondiales majeures. Les menaces cybernétiques deviennent de plus en plus sophistiquées, les atteintes massives à la protection des données sont communes et, en raison des cyber-attaques de type Advanced Persistent Threat, APT), quasi n'importe qui pourrait en être une cible ; de plus, avec l'« Internet des Objets », les appareils « intelligents » omniprésents dans nos environnements pourraient être utilisés en tant qu'arme de déni de service distribué (Distributed Denial of Service, DDoS).

Dans le cadre des services financiers, ces acteurs représentent une menace cybernétique où la principale motivation de la victime est le **vol d'actifs**.

Mais, naturellement, les organisations faisant partie de l'écosystème bancaire et de paiement n'exercent pas leurs activités en vase clos : elles interagissent et effectuent quotidiennement des transactions avec leurs multiples contreparties. Le risque est réel, car les cyber-attaques ciblant les clients de SWIFT de la part d'un petit nombre d'acteurs sophistiqués et bien financés continuent. **Comment une organisation devrait-elle envisager et adresser son risque potentiel d'effectuer des transactions avec une victime involontaire d'une cyber-attaque ?** Si le risque n'est pas géré, et les fonds sont perdus, le risque financier peut être important.

Les présentes directives examinent comment une organisation pourrait aborder l'évaluation des risques cybernétiques que leurs contreparties représentent et couvrent quatre domaines clés :

- Définir un modèle de gouvernance pour la gestion des risques cybernétiques
- Définir un cadre de gestion des risques cybernétiques
- Adopter des contre-mesures d'atténuation des risques liés cybernétiques
- Intégrer les données d'attestation de cybersécurité des contreparties de SWIFT

Le reste de ce document examine ces quatre sujets.

Voix du client

Les données d'attestation de cybersécurité vous ont-elles aidé à traiter un ou plusieurs de ces défis et, si c'est le cas, comment ?

« Le processus d'attestation de la sécurité des clients de SWIFT a complété notre programme global de gestion de nos membres pour contribuer à traiter ces défis. Avec ces données d'attestation, nous pouvons maintenant comprendre le niveau de contrôle de sécurité mis en œuvre par des contreparties. En ayant une bonne compréhension du type et du niveau de contrôles déployés chez chaque contrepartie, nous sommes en meilleure position pour gérer le cyber-risque.

Le programme CSP de SWIFT nous a fourni un ensemble cohérent de réponses fournies par toutes les contreparties et qui peut être exploité pour définir des indices de référence. C'est pour nous ce que le test SAT (Standard Aptitude Test – Test standard d'aptitude) est pour les équipes d'admission à l'université. L'outil d'attestation est très facile à utiliser pour demander et accorder l'accès aux données de cybersécurité aux contreparties. Le programme CSP de SWIFT améliore la confiance que nous avons dans les réponses fournies par les contreparties en donnant aux contreparties un moyen de faire valider leurs réponses par un audit interne et/ou externe. Nous avons développé un modèle quantitatif pour utiliser les données à partir de l'outil d'attestation et générer des rapports et tableaux. »

Définir un modèle de gouvernance pour la gestion des risques cybernétiques

Les risques cybernétiques, y compris ceux auxquels les contreparties sont exposées, doivent être gérés en combinaison avec d'autres types de risques : opérationnels, financiers et réglementaires.

La supervision de ce processus de gestion des risques – la gouvernance – doit être organisée de manière à ce que les personnes compétentes qui assument des responsabilités adéquates soit à même de prendre des décisions, que les processus soient robustes et répétables, et que les exceptions soient gérées de manière adéquates

Structure du Comité de supervision

La gouvernance des risques cybernétiques devrait être considérée comme étant une fonction holistique. Cela signifie qu'elle devrait être centralisée, entre les mains de ceux qui sont responsables des activités globales de l'entreprise, au lieu d'être confinée à une fonction de back-office isolée des Technologies de l'information (TI) ou de l'Exploitation. Dans la pratique, la gestion du risque des contreparties devrait faire partie (ou être un sous-ensemble) d'une **structure de Comité de supervision, tel qu'un Comité de gestion des risques,** ayant son propre mandat et doté de ressources suffisantes.

Dans le cadre de cette gouvernance interdisciplinaire, il faudra également s'assurer d'un alignement des responsabilités au travers des « 3 lignes de défense ». Dans la pratique, cela signifie que les décisions relatives au risque opérationnel prises quotidiennement devraient s'effectuer au niveau de la première ligne (p. ex., activités commerciales, exploitation, TI/cyber) étant donné que ses membres sont responsables de l'exécution des contrôles internes et des procédures opérationnelles. Les exceptions et l'information des niveaux supérieurs devraient être gérées au niveau de la deuxième ligne de défense (p. ex., comités de conformité, risque) étant donné que ses membres jouissent d'une certaine indépendance opérationnelle. L'assurance relative à la conformité devrait être supervisée par la troisième ligne de défense (p. ex., audit interne) étant donné que ses membres sont indépendants.

Parties prenantes commerciales

Les fonctions de gouvernance devraient être confiées aux personnes qui ont des niveaux d'ancienneté suffisants et qui sont habilités à prendre des décisions ayant un impact parmi les groupes de parties prenantes internes appropriés.

On pourrait prétendre que bon nombre de décisions liées au risque opérationnel pour la gestion des contreparties, et prises quotidiennement, devraient provenir des **commerciaux** plutôt que des personnes des fonctions strictement techniques ou de cybersécurité. Cependant, la gouvernance globale doit être holistique et inclure des représentants des fonctions suivantes :

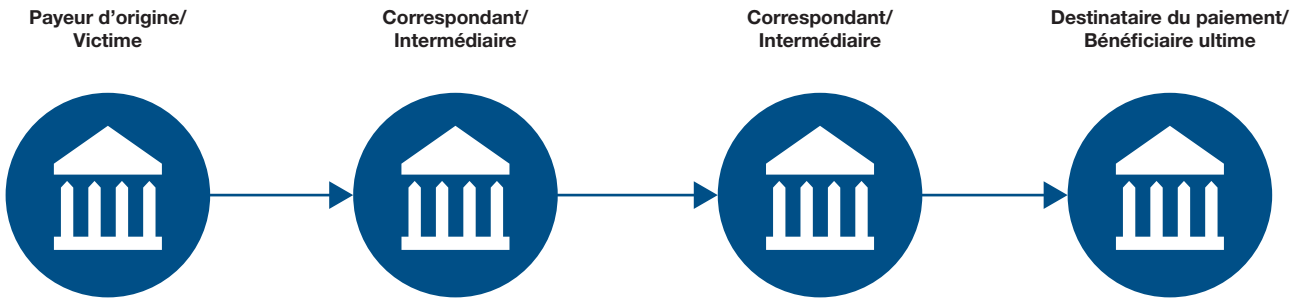
- **la gestion des relations commerciales** et des contreparties, pour évaluer les risques de marché et des contreparties et faire la liaison avec la contrepartie ;
- **les opérations de paiement,** pour mettre en œuvre les contrôles opérationnels, ajuster les limites et intervenir dans les activités opérationnelles habituelles ;
- **les fonctions techniques,** p. ex., TI/ sécurité de l'information/cybersécurité, pour introduire des contrôles techniques complémentaires ou des mesures ciblées de détection de la fraude ;
- **le risque, la conformité et l'audit,** pour gérer les exceptions et fournir une assurance de conformité indépendante.

En raison de la sensibilité des données et de l'impact potentiel des incidents en matière de sécurité, un haut responsable devrait superviser ce processus, aider à piloter l'évaluation des risques et le processus de soumission à un palier supérieur, et surveiller les décisions qui en découlent en matière de contre-mesures.

Mandat précis

Le Comité supérieur supervisant le risque de contrepartie devrait avoir un mandat clairement énoncé ou des termes de référence qui décrivent la stratégie à plus long terme, ainsi que le modèle opérationnel quotidien, y compris les rôles et responsabilités.
Ce mandat devrait également inclure la nécessité de faire régulièrement des comptes rendus au Conseil d'administration et à la haute direction sur le paysage du risque cybernétique des contreparties, les incidents spécifiques, et leur évolution et tendances.

Cadre d'évaluation du risque cybernétique des contreparties



Le présent guide s'adresse aux :

- **Petites et moyennes entreprises** qui reçoivent des instructions de la part d'un payeur. Ces PME ont un nombre limité de contreparties, en comparaison avec les grandes institutions qui ont des relations avec de nombreuses contreparties et des structures internes complexes ;
- **Correspondants bancaires** (indifféremment de leur taille) qui agissent en tant qu'intermédiaires de la transaction entre le payeur d'origine et le bénéficiaire ultime.

Voix du client

Pouvez-vous décrire concrètement comment vous utilisez vos données d'attestation de cybersécurité, en plus de simplement soumettre votre auto-attestation dans l'outil ; plus précisément, comment vous les utilisez dans le contexte de la gestion du risque en matière de sécurité pour vos contreparties ?

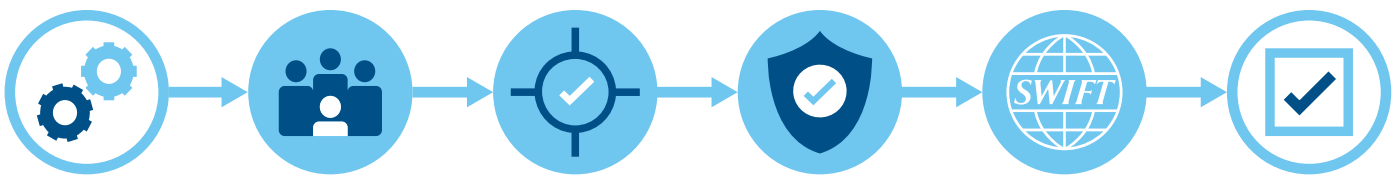
« L'outil d'attestation fournit des réponses cohérentes, de sorte que nous pouvons évaluer chaque attestation et appliquer une valeur numérique sur la base des réponses. Cela nous a permis d'appliquer des mesures quantitatives et qualitatives à chaque attestation. Auparavant, nous nous en remettions uniquement à des questionnaires qui fournissaient souvent des réponses incohérentes. »

Définir un cadre de gestion des risques cybernétiques

En instaurant une structure de gouvernance robuste, les institutions aborderont généralement la cybersécurité sous l'angle du risque. Cela signifie qu'elles évaluent le niveau de risque, investissent un budget là où il est le plus nécessaire, et acceptent les risques lorsqu'ils se situent en-dessous d'un seuil ou d'un niveau appétit. Le processus, ou cadre, de gestion des risques cybernétiques comprend plusieurs étapes :

1. **Recueillir les données nécessaires sur le risque des contreparties**
2. **Évaluer le niveau du risque en traitant les données. Ce travail s'effectue généralement en attribuant une note globale, puis en l'appréciant par rapport au niveau d'appétit de la société pour le risque**
3. **Sur la base de la note de risque, mettre en œuvre des mesures appropriées pour gérer ou « adresser » les risques**

Cadre d'évaluation du risque cybernétique des contreparties



Définir un modèle de **gouvernance** pour la gestion des risques cybernétiques

Définir un cadre de **gestion des risques** cybernétiques

Adopter des **contre-mesures** d'atténuation des risques cybernétiques

Intégrer les **données d'attestation** de cybersécurité des contreparties de SWIFT

Données relatives aux risques des contreparties

Les institutions recueillent et traitent diverses données pour contribuer à définir le profil de risque des contreparties sur l'angle cybernétique

Les données sur les risques peuvent être ventilées en trois catégories : données liées à l'environnement externe dans lequel la contrepartie exerce ses activités ; données qui décrivent la relation commerciale avec la contrepartie ; et données transactionnelles :

1. Données liées à l'environnement externe dans lequel la contrepartie exerce ses activités

- **Pays/Région des activités** – celles-ci pourraient servir de mesure du niveau de cybersécurité, réglementation et crime/fraude dans la juridiction dans laquelle la contrepartie exerce ses activités. Cela peut être évalué en utilisant les sources disponibles publiquement, telles que le rapport de Bâle sur les risques en matière de lutte contre le blanchiment de capitaux
- **Type d'industrie** – celles-ci pourraient être mises en relation avec la probabilité d'être attaqué, car certains secteurs sont plus souvent que d'autres victimes d'attaques cybernétiques et de vols de données
- **Niveau de supervision réglementaire** de la contrepartie et mesure dans laquelle le superviseur local impose la réglementation ou la politique relative à la cybersécurité

2. Risques liés à la relation commerciale avec la contrepartie

- **Niveau/Durée de la relation avec la contrepartie** – les nouvelles relations pourraient présenter un risque plus élevé qu'une relation de longue date, profonde et de confiance
- **Taille/Structure d'actionnariat de la contrepartie** – celles-ci pourraient être corrélées à la disponibilité du budget, aux qualifications du personnel et aux outils pour combattre les menaces, particulièrement si la contrepartie est rattachée à un plus grand groupe, p. ex., Global Systemically Important Banks (GSIB – Banques d'importance systémique au niveau mondial)
- **Incidents cybernétiques ou de sécurité connus** ou autres nouvelles, informations ou matériaux de diligence raisonnable disponibles
- **Évaluations des risques existants pour la contrepartie,** p. ex., opérationnel, financier ou réglementaire

3. Risques liés aux transactions

- **Types de transactions** – limiter le type de transactions effectuées avec la contrepartie car certains types de transactions sont, par nature, plus vulnérables que d'autres, p. ex., les paiements vs les relevés
- **Valeur de la transaction** – représente le risque de crédit
- **Fréquence de la transaction** – plus le volume de transactions est élevé par période, et plus élevé est le risque de voir des attaques.

Une fois que les données sur la contrepartie ont été rassemblées, le processus d'évaluation des risques peut être appliqué.

Processus d'évaluation des risques

Une fois que les données sur la contrepartie ont été recueillies, les institutions les traitent et les transforment en une évaluation basée sur les risques. La méthodologie d'évaluation peut différer parmi les institutions mais, généralement, elle suit l'une de ces trois approches :

- **Basée sur l'expertise** – où l'évaluation relève d'un jugement d'experts et d'une évaluation qualitative des risques par des spécialistes
- **Basée sur la règle** – où l'évaluation s'effectue par le biais d'un arbre de décision en utilisant des règles simples basées sur les notes obtenues par la contrepartie par rapport à chaque facteur de risque
- **Basée sur le modèle** – où l'évaluation provient d'une analyse des notes obtenues par la contrepartie par rapport à chaque facteur de risque pondéré

Quelle que soit l'approche adoptée, généralement, une note globale est attribuée à la contrepartie, sous la forme d'un indicateur rouge, orange ou vert.

Les contre-mesures d'atténuation des risques seraient fonction de cette note en tenant compte de l'appétit interne en matière de risque. Par exemple, les contreparties ayant une note peu élevée (couleur verte) peuvent être classifiées comme ne nécessitant pas de contrôles supplémentaires, mais les contreparties ayant une note élevée (couleur rouge) peuvent être sélectionnées pour la prise de contre-mesures d'atténuation des risques.

Adopter des contre-mesures d'atténuation des risques cybernétiques

Le cadre de gestion des risques peut permettre à une institution d'évaluer et de classifier le niveau de risque associé à une contrepartie en matière de sécurité. L'institution peut ensuite prendre une décision, à savoir, soit accepter les risques, ou envisager de prendre des contre-mesures d'atténuation des risques.

Les contre-mesures d'atténuation des risques cybernétiques peuvent englober :

1. Contre-mesures liées à la relation commerciale avec la contrepartie

- **Sensibilisation proactive de la haute direction** pour renforcer la relation et réassurer de manière générale
- Demandes à la contrepartie de **justifier ses informations** par le biais d'une évaluation interne ou de tiers/externe, ou en fournissant des documents de spécifications techniques ou des résultats de tests
- Demandes à la contrepartie de mettre en œuvre des **contrôles supplémentaires** ou des mesures de **détection de la fraude**
- Réévaluation des **accords et contrats** conclus avec la contrepartie, y compris la possibilité d'« éliminer le risque » de contrepartie et changer ou résilier le contrat

2. Contre-mesures liées à une gouvernance transactionnelle plus rigoureuse avec la contrepartie

- Baliser pour examen les transactions qui violent les **seuils prédéfinis**. Il peut s'agir du type de transaction, de la valeur de la transaction, de la devise de la transaction, ou du profil du bénéficiaire ultime
- Pour toutes les transactions balisées, mettre en œuvre des **contrôles supplémentaires**, p. ex., une supervision manuelle selon le principe des « quatre-yeux » et/ou une vérification bilatérale de la transaction avec la contrepartie

La liste précédente de contre-mesures n'est pas destinée à être exhaustive et les institutions peuvent déployer d'autres contrôles et outils pour contribuer à gérer le risque.

Appliquer des contre-mesures pour les contreparties à risque élevé

Pour les contreparties à risque élevé, les institutions peuvent souhaiter appliquer une combinaison des contre-mesures précitées. Généralement, une institution souhaite appliquer des contrôles supplémentaires et surveiller les instructions en matière de paiement pour une valeur ou un seuil de volume prédéfini(e). L'institution devrait pouvoir ajuster les seuils et, également, les outils et la capacité de gérer un nombre accru d'alertes, ainsi que les efforts supplémentaires requis pour traiter manuellement la transaction, y compris le fait de devoir obtenir des coordonnées actualisées de la contrepartie.

Ces contrôles accrus n'ont pas nécessairement besoin d'être maintenus en permanence. Dès que la contrepartie réussit à être re-classifiée dans la catégorie de risque « peu élevé », p. ex., parce qu'elle se conforme aux contre-mesures supplémentaires, les seuils peuvent être altérés ou supprimés.

Au-delà de toute décision de mettre en œuvre des contre-mesures d'atténuation, chaque institution demeure entièrement et exclusivement responsable d'altérer, de mettre en suspens ou de résilier, en tout ou en partie, la relation avec la contrepartie.

Une fois que le processus de gestion des risques cybernétiques a été mis en place, il est prudent pour la structure de gouvernance d'effectuer des examens périodiques de la contrepartie pour évaluer si son profil de risque a changé.

Voix du client

Comment les données d'attestation de cybersécurité s'inscrivent-elles dans la gestion des risques cybernétiques et quels organes de gouvernance sont constitués en la matière ?

« Des rapports hebdomadaires sont communiqués à notre directeur de la gestion des risques, et à d'autres départements de la gestion des risques. Nous suivons le nombre de demandes d'accès aux attestations acceptées en le comparant au nombre de demandes d'accès aux attestations en attente. Pour les demandes d'accès aux attestations acceptées, nous notons chaque attestation en matière de risque, puis nous associons chaque attestation notée au profil qualitatif. Nos départements de la gestion des risques ont commencé d'intégrer les résultats des profils dans leurs disciplines. »

Annexe A : Intégrer les données d'attestation des contreparties de SWIFT

Lancé en mai 2016, le Customer Security Programme (CSP – Programme relatif à la sécurité des clients) de SWIFT apporte un soutien à tous les segments d'utilisateurs de SWIFT pour renforcer la sécurité de leur infrastructure SWIFT locale.

La Customer Security Controls Policy (CSCP – Politique relative aux contrôles de sécurité des clients) définit le processus d'attestation des utilisateurs et les principes, rôles et responsabilités y afférents. SWIFT a également développé un Customer Security Control Framework (CSCF – Cadre des contrôles de sécurité des clients) qui définit des données de base en matière de sécurité pour les contrôles obligatoires et recommandés à l'intention de toute la communauté d'utilisateurs.

La Politique CSCP exige que les utilisateurs évaluent eux-mêmes leur conformité à un ensemble de **contrôles obligatoires en matière de sécurité**, et elle les encourage également à évaluer eux-mêmes leur conformité à un ensemble de contrôles recommandés. Ils attestent de leur niveau de conformité, et leur **attestation** est publiée et gérée par le biais de l'application KYC- Security Attestation (KYC-SA – Connaître son client-Attestation en matière de sécurité) que SWIFT leur fournit.

Une fonctionnalité clé de l'outil KYC-SA est la possibilité pour les institutions d'échanger les données d'attestation avec leurs contreparties, par accord mutuel, **« en demandant » ou « en acceptant » l'accès**. Ce faisant, les institutions peuvent évaluer le risque d'une contrepartie, puis prendre des décisions en matière de risque de contrepartie sur la base des niveaux de conformité attestés. Ces données d'attestation sont riches en informations et une source unique de données sur le risque de la contrepartie en matière de cybersécurité.

Tandis que les institutions commencent à intégrer leurs données d'attestation CSP dans leurs cadres du risque des contreparties, un certain nombre de facteurs doivent être pris en compte :

- Réflexions sur le modèle de gouvernance
- Réflexions sur le cadre de gestion des risques
- Autres options pour les contre-mesures d'atténuation

Ces trois domaines de réflexion sont examinés ci-dessous dans le cadre général de l'outil KYC-SA.

Il est important de souligner que les utilisateurs auteurs des attestations sont seuls responsables de l'exactitude de leurs attestations et que SWIFT ne valide pas cette exactitude. Le CSP est destiné à créer un niveau de **normalisation** et de **transparence** pour les informations sur la sécurité qui sont partagées et qui peuvent ensuite être exploitées par les utilisateurs de SWIFT.

Veuillez remarquer que l'Annexe B renferme des liens vers les documents sur le Cadre CSCF et la Politique CSCP.

L'Annexe B renferme également des liens vers les Directives à l'intention de l'utilisateur KYC-SA . Ces directives indiquent pas à pas comment demander/accepter l'accès aux données d'attestation et comment exporter les données d'attestation sous forme de fichier Excel. Le responsable de la gestion de la sécurité de l'organisation peut exporter les données d'attestation pour chaque contrepartie, ou en vrac, parmi toutes les contreparties pertinentes. Cependant, ces directives ne vont pas jusqu'à décrire comment une organisation devrait utiliser les données, c.-à-d. définir la gouvernance, traiter les données, évaluer le risque et prendre des contremesures. Ces conseils sont décrits ci-dessous.

Voix du client

Comment fonctionne votre gouvernance pour accepter les demandes d'accès de contreparties à vos données d'attestation ? Est-ce une responsabilité partagée (p. ex., entre la Gestion du risque, la Conformité, le Juridique, etc.) ?

« Le processus de gouvernance pour accepter les demandes d'accès des contreparties à nos données d'attestation requiert la participation de plusieurs équipes. Pour assurer la transparence de l'acceptation des demandes d'accès à nos attestations. Nous avons un processus interne d'approbation des demandes relatives aux attestations Une fois l'approbation obtenue au niveau interne, l'équipe administrative accepte la demande d'accès dans l'outil d'attestation. »

Réflexions sur le modèle de gouvernance

Avant de décider de partager les données d'attestation, ou demander à d'autres de partager les leurs, le processus global d'utilisation des attestations de contreparties doit être défini. Plus précisément, il convient d'inclure la manière dont le partage aura lieu, et indiquer qui doit remplir ce rôle.

Bien que SWIFT fournisse la plateforme technique, le modèle de gouvernance de l'institution doit également être adapté pour apporter un soutien à l'évaluation des données d'attestation de la contrepartie en matière de sécurité. Des représentants compétents choisis dans tous les métiers pertinents de l'institution devraient être envisagés pour « accepter » ou « demander » l'accès aux données d'attestation, et les données devraient être considérées comme étant un élément supplémentaire faisant partie du cadre déjà existant dans l'organisation de la gestion du risque des contreparties

Accepter (ou refuser) les demandes d'accès des contreparties

Pour accepter la demande d'accès d'une contrepartie, le modèle de gouvernance doit clairement identifier le responsable de l'entreprise qui gère le processus décisionnel consistant à dire « oui » ou « non ». En l'absence de la nomination d'un « responsable d'acceptation », les demandes d'attestation reçues seront mises en file d'attente et laissées sans réponse.

Généralement, les critères relatifs à la décision d'approbation utilisés pour accepter les demandes d'accès reçues devraient être approuvés par écrit par un comité de direction, tel que le Comité de gestion des risques, ou par un membre de la direction générale, tel que le responsable de la sécurité des systèmes d'information (RSSI), le directeur des Affaires juridiques ou le directeur de la gestion de la conformité.

Exemples de critères de décision utilisés par le« responsable d'acceptation » pour accepter les demandes d'accès de contreparties

- Les données d'attestation seront partagées avec les banques de transactions mondiales, indépendamment de leur localisation géographique.
- Les données d'attestation seront partagées avec les contreparties situées dans la même zone géographique et supervisée par le même régulateur.
- Les données d'attestation seront partagées une fois que nous pourrons indiquer dans le champ « Type d'attestation » de notre attestation que celle-ci est confirmée par une évaluation ou un audit externe.
- Les données d'attestation seront partagées avec toutes les contreparties qui les demandent et avec lesquelles nous entretenons des relations actives de messagerie.
- Les données d'attestation seront partagées avec toutes les contreparties qui les demandent et qui communiquent également leurs données d'attestation à notre institution.
- Les données d'attestation seront partagées avec toutes les contreparties qui les demandent.

La structure de Comité de direction ou la direction générale devrait approuver par écrit les critères de décision. Une fois l'approbation obtenue, la direction de niveau intermédiaire peut alors appliquer les critères aux demandes reçues et communiquer aux opérateurs techniques la décision d'accepter ou de refuser la demande d'accès.

Les exceptions devraient faire l'objet d'une soumission à la structure de Comité supérieur ou la direction générale.

Au niveau opérationnel, les opérateurs (ou « responsables d'acceptation ») devraient communiquer sur une base régulière (p. ex., chaque semaine) un résumé des demandes reçues, et les mesures prises, à la direction,

Exemple de processus pour accepter les demandes d'accès

1. Attribuer le rôle de « responsable d'acceptation » à un opérateur
2. L'opérateur reçoit une demande d'accès de la part d'une contrepartie.
3. L'opérateur examine la demande par rapport aux critères d'approbation et recommande une réponse positive ou négative.
4. La direction de niveau intermédiaire examine la recommandation et permet d'exécuter, de communiquer une autre décision ou soumet le cas à la direction générale.
5. L'opérateur « accepte » ou « refuse » la demande d'accès de la contrepartie. En cas de refus, l'opérateur devrait être en mesure de justifier le refus. Le refus pourrait être dû, p. ex., à l'absence de relations avec la contrepartie ou au fait de ne pas être prêt à partager les données d'attestation pour le moment.
6. L'opérateur communique un résumé du statut des demandes et des mesures prises sur une base régulière, p. ex., chaque semaine.

L'outil d'attestation fournit également la possibilité de créer une « liste blanche » des BIC (Business Identifier Code, code d'identification d'entreprise) des contreparties qui répondent aux critères définis par la direction générale. Il serait ainsi possible d'accepter automatiquement les demandes d'accès de ces contreparties, sans devoir procéder à des examens et approbations manuels. Cette fonctionnalité est également connue sous le nom d'« auto-acceptation ».

Demande d”accès de la part de contreparties

La structure de Comité direction ou la direction générale devrait approuver par écrit les critères d’acceptation des demandes d’accès des contreparties. Les critères de demande d’accès aux données d’attestation des contreparties devraient être décidés à un niveau similaire de direction.

Exemples de critères de décision utilisés par le « demandeur » pour demander d’accéder aux données de contreparties

- Nous demanderons des données d’attestation de la part de toutes nos contreparties.
- Nous demanderons des données d’attestation uniquement de la part des contreparties avec lesquelles nous ne sommes pas régulièrement en relation.
- Nous demanderons des données d’attestation uniquement de la part des contreparties qui résident dans une région à risque élevé.
- Nous demanderons des données d’attestation uniquement des contreparties qui sont déjà considérées comme présentant un risque élevé.

Une fois que la direction générale a défini les critères de décision, les demandes d’attestation devraient être exécutées dans l’outil d’attestation par un opérateur (« demandeur »).

Le statut des demandes d’accès aux données d’attestation des contreparties devrait être communiqué à la direction sur une base régulière (p. ex., chaque semaine), tout comme le statut de l’acceptation des demandes d’accès des contreparties est communiqué.

Exemple de processus pour demander l’accès

1. Attribuer le rôle de « demandeur » à un opérateur.
2. La direction générale définit les critères de décision pour demander d’accéder aux données d’attestation des contreparties.
3. L’opérateur envoie la demande à la contrepartie en utilisant l’outil d’attestation.
4. La contrepartie « accepte » ou « refuse » la demande d’accès. Si la demande est refusée, la direction générale devrait envisager de recontacter la contrepartie et redemander l’accès après que la raison du refus ait été traitée.
5. L’opérateur communique un résumé du statut des demandes et des mesures prises sur une base régulière, p. ex., chaque semaine.

Voix du client

Lorsque vos demandes d’accès aux données d’attestation de contreparties ont été acceptées, vous est-il arrivé de recevoir des informations qui vous ont incité à prendre une décision importante en matière de cybersécurité ? Si c’est le cas, pouvez-vous en parler ?

« Une fois que notre demande d’accès aux données d’attestation d’une contrepartie est acceptée, nous examinons les réponses aux contrôles. Nous n’avons cependant pas pris de décisions en matière de cybersécurité sur la base d’une attestation de contrepartie. Les réponses des contreparties ont alimenté nos conversations internes sur la contagion cybernétique. »

Réflexions sur le cadre de gestion des risques

Les organisations dont la demande d'accès aux données d'attestation d'une contrepartie a été acceptée peuvent se servir de l'outil pour « utiliser » ces données. Ces données d'attestation, qui englobent les niveaux de conformité par contrôle, devraient être intégrées dans le cadre décisionnel des organisations basé sur les risques, et contribuer à gérer le risque que représente la contrepartie.

Les institutions qui souhaitent intégrer les données d'attestation de cybersécurité dans leur processus de gestion des risques existant pourraient estimer utile d'appliquer des pondérations et des notes sur la base de ces informations.

Exemple d'approche pour les pondérations et les notes

- Si la contrepartie n'a pas attesté, il convient de la noter.
- Si la contrepartie n'a pas répondu aux demandes d'accès KYC-SA, il convient de la noter.
- Les niveaux de conformité pour chaque contrôle CSCF devraient être notés : p. ex., la conformité selon le Guide de mise en œuvre SWIFT, la conformité selon d'autres moyens, le manque de conformité ou la conformité future à une date donnée.
- Chaque contrôle spécifique, obligatoire ou recommandé, peut se voir attribuer une pondération différente.
- D'autres variables d'attestation peuvent recevoir une pondération spécifique, p. ex. :
  - **Type d'infrastructure**
  - **Composantes de l'infrastructure** : la contrepartie utilise-t-elle une interface certifiée ?
  - **Prestataire de service** : la contrepartie se connecte-t-elle par le biais d'un prestataire de service et quel est le statut de ce prestataire en matière de certification ou de conformité ?
  - **Type d'évaluation** : la contrepartie a-t-elle engagé un tiers interne ou externe pour être conseillée, ou son attestation a-t-elle été justifiée par une évaluation indépendante interne ou externe ? Voir ci-dessous

L'attribution de pondérations et de notes significatives est un exercice méticuleux pour lequel les institutions devraient assurer la collaboration entre les parties prenantes internes, p. ex., celles de la sécurité des systèmes d'information, de l'exploitation, de la technologie, de la gestion du risque, de la conformité, des activités commerciales et du juridique.

Interpréter le « Type d'évaluation »

Ce champ de l'auto-évaluation saisit la mesure dans laquelle la contrepartie a utilisé des examinateurs indépendants pour justifier son niveau attesté de conformité.

– **Évaluation indépendante de tiers (qui peut inclure un audit par un auditeur externe)** : l'institution a validé la conformité aux contrôles en utilisant un évaluateur externe indépendant. Son nom doit être indiqué par l'institution qui fournit l'attestation. – **Évaluation indépendante interne (qui peut inclure un audit interne)** : l'institution a validé la conformité aux contrôles en utilisant une fonction d'évaluateur interne.	Est susceptible de permettre un niveau plus élevé d'assurance de conformité raisonnable indiquant que le statut de conformité attribué à chaque contrôle a été vérifié de manière indépendante. Est susceptible d'impliquer un niveau de confiance plus élevé pour les contreparties qui peuvent fournir ce niveau d'assurance de conformité. Permet de vérifier le nom de l'évaluateur externe.
– **Examen consultatif par une entreprise externe** : l'institution a engagé un tiers pour se faire conseiller dans le cadre de l'évaluation de sa conformité. Le nom du tiers doit être indiqué par l'institution qui fournit l'attestation. – **Examen consultatif par des équipes indépendantes internes** : l'institution a engagé une entité interne indépendante pour se faire conseiller dans le cadre de l'évaluation de sa conformité.	Est susceptible de fournir un certain niveau de confiance dans la vérification indépendante du statut du contrôle indiqué. Les évaluations consultatives ne se déroulent pas selon un cadre fixe, prédéfini. La confiance peut être renforcée en établissant un rapport d'évaluation complet et en le mettant à disposition. Pourrait être complété par une évaluation ciblée ou un contrôle d'échantillon.
– **Auto-évaluation** : l'institution a auto-évalué ses déclarations, p. ex., par le biais de l'approbation par écrit du RSSI, du directeur de la gestion des risques ou d'autres rôles de direction.	Est susceptible d'établir un niveau minimal de confiance indiquant que la contrepartie a évalué à fond sa conformité aux contrôles CSCF.

Autres contre-mesures d'atténuation des risques

Au-delà des contre-mesures génériques décrites dans la section 4, la réflexion pourrait être étendue pour inclure un certain nombre d'options supplémentaires propres à l'utilisation de SWIFT, comme indiqué ci-dessous.

Demander de se conformer aux contrôles recommandés

En dehors de l'obligation actuelle de s'auto-évaluer par rapport à l'ensemble des contrôles obligatoires, les institutions pourraient estimer utile de demander que certaines contreparties s'auto-évaluent également par rapport aux contrôles recommandés, en tout ou en partie.

Utilisation de mesures de détection de la fraude par les contreparties

Les utilisateurs SWIFT pourraient estimer utile de demander que certaines contreparties mettent en œuvre des capacités de détection de la fraude qui recherchent les anomalies ou valeurs aberrantes et qui ne représentent pas un schéma de comportement normal. Cela est actuellement défini en tant que « Advisory Control » (Contrôle conseillé) dans CSCF v2019.

Exemple : Daily Validation Report (DVR – Rapport de validation journalier) SWIFT

Dans le cadre de son programme CSP, SWIFT a renforcé son portefeuille d'outils relatifs à la conformité en matière de crime financier en y ajoutant un outil de d'observation des schémas transactionnels. Le but est d'atténuer le risque associé à la fraude en matière de paiement.

Le Rapport de validation journalier (DVR) permet aux institutions de pouvoir facilement valider l'activité des transactions de paiement, mettre en lumière les risques potentiels, et réagir rapidement en cas de fraude.

Le rapport DVR fournit des informations sur les activités de paiement du jour précédent. Les totaux des valeurs et des volumes des transactions quotidiennes sont comparés aux moyennes des valeurs et des volumes journaliers de l'utilisateur au cours des 24 mois précédents, permettant d'identifier et de comprendre rapidement tout changement significatif de l'activité.

Deux domaines clés sont couverts :

- Le Rapport d'activité permet aux utilisateurs de voir leurs activités journalières agrégées : l'activité journalière agrégée est fournie par type de message, devise, pays et contrepartie. Les totaux des valeurs et des volumes quotidiens sont également fournis ainsi que des données sur les transactions les plus importantes.
- Le Rapport sur les risques est destiné à faire ressortir les flux de messages importants ou inhabituels pouvant indiquer des risques de fraude. Il aide les utilisateurs à sélectionner la ou les transactions individuelles les plus importantes et les plus gros flux de transactions agrégées avec leurs contreparties pour les paiements entrants et sortants. Les comparaisons avec les totaux des valeurs et des volumes quotidiens moyens précédents permettent aux utilisateurs d'évaluer les changements d'activité. Le Rapport sur les risques fait également apparaître toutes nouvelles combinaisons de contreparties directes ou indirectes provenant des transactions du jour concerné.

Les informations sont agrégées pour les types de messages SWIFT clés suivants : MT 103, MT 202, MT 202COV, MT 205 et MT 205COV.
DVR a été lancé en 2016.

Exemple : Payment Controls Service (PCS – Service de contrôles des paiements) SWIFT

Le Service de contrôles des paiements (PCS) s'applique spécifiquement à aider les utilisateurs SWIFT à détecter les activités irrégulières en cours. PCS détecte en temps réel et pendant leur déroulement, les paiements non-conformes pour une contrepartie, ou qui sont anormaux et indicatifs d'un risque de fraude. Il s'effectue hors bande, c.-à-d. à l'extérieur des locaux de l'utilisateur. Cela implique que même si l'institution est victime d'un incident cybernétique, les données demeurent fiables.

PCS fonctionne selon l'un de deux modes opérationnels en temps réel en utilisant les règles définies par le souscripteur :

- Copier le message et alerter ; ou
- Mettre en attente le message et alerter.

Dans son essence, le service PCS permet aux utilisateurs de configurer des règles parmi un certain nombre de paramètres :

- Calendriers des jours ouvrables, jours non-ouvrables et heures de bureau habituelles
- Listes blanches/Listes noires des devises, limites des paiements individuels et agrégés
- Listes blanches/Listes noires des pays, limites des paiements individuels et agrégés
- Seuils définis pour le pays, la devise, l'entité individuelle ou leurs combinaisons
- Nouvelles institutions : identifier les paiements avec de nouveaux participants ou chaînes, sur la base des flux de messages historiques
- Comptes suspects : vérifier les numéros de compte du client ultime par rapport à la liste noire des numéros de compte estimés présenter un risque élevé d'une institution

PCS a été lancé en octobre 2018.

Veuillez remarquer qu'avant qu'une institution ne mette en œuvre des contrôles de fraude au niveau du bénéficiaire ou avant qu'une institution ne demande à une contrepartie de mettre en œuvre des contrôles de fraude au niveau de l'expéditeur, les Conditions générales et d'autres considérations juridiques devraient être examinées.

Affiner la relation et la mettre en vigueur avec RMA (Relationship Management Application – Application de gestion des relations)

Les relations instaurées il y a plusieurs années sont susceptibles d'avoir changé au fil du temps et de ne plus être alignées sur les schémas commerciaux actuels. En plus de contrôler qui peut envoyer des messages avec l'application RMA, les utilisateurs SWIFT peuvent limiter les types de messages avec RMA+. Par exemple, un utilisateur peut accepter de recevoir des messages de trésorerie ou d'opérations commerciales, mais pas des messages de paiement.

Exemple : RMA et RMA Plus SWIFT

L'Application de gestion des relations (RMA) est le principal processus d'échange et d'autorisation entre deux institutions financières et permet aux institutions de définir quelles contreparties peuvent leur envoyer des messages FIN. Tout trafic indésirable est bloqué au niveau de l'expéditeur, limitant les risques opérationnels associés à la manipulation des messages indésirables.

RMA Plus, version plus granulaire de RMA, va plus loin en permettant aux institutions de spécifier le type de message ou les types de messages qu'elles souhaitent envoyer à chacune de leurs contreparties, et recevoir de la part de chacune de leurs contreparties. Par exemple, une institution pourrait uniquement souhaiter recevoir des lettres de crédit d'un correspondant spécifique.

Les institutions doivent donner des autorisations RMA ou RMA Plus à leurs contreparties pour recevoir des messages de la part de ces contreparties, et la fonctionnalité RMA est intégrée dans les interfaces Alliance Access et Alliance Entry SWIFT.

Au fil du temps, de nombreuses institutions ont mis en place plusieurs relations RMA avec un grand nombre de contreparties. Cependant, la liste des autorisations RMA risque de ne pas avoir toujours été actualisée lorsque les relations commerciales changent ou ont été résiliées. Par conséquent, les institutions sont susceptibles d'avoir un grand nombre de règles RMA inactives en place, et risquent même de ne pas le savoir.

En rationalisant et en révoquant les règles RMA dormantes ou inactives, les institutions peuvent minimiser le temps et les coûts associés à de telles activités, et limiter les risques..

Les institutions peuvent entreprendre cette tâche de rationalisation elles-mêmes. Sinon, SWIFT propose un service de « nettoyage » des autorisations RMA et RMA Plus.

L'application RMA a été lancée en 2009.

Annexe B : Glossaire

Terme	Acronyme	Description
Customer Security Programme (Programme relatif à la sécurité des clients) SWIFT	CSP	**Cliquez ici pour en savoir davantage.**
Customer Security Control Framework (Cadre des contrôles de sécurité des clients)	CSCF	**Cliquez ici pour en savoir davantage.**
Customer Security Control Policy (Politique relative aux contrôles de sécurité des clients)	CSCP	**Cliquez ici pour en savoir davantage.**
Know Your Customer-Security Attestation (Connaître son client-Attestation en matière de sécurité) (application)	KYC-SA	Données de base : **Cliquez ici pour en savoir davantage.** Guide de l'utilisateur : **Cliquez ici pour en savoir davantage.**
Relationship Management Application (Application de gestion des relations)	RMA	**Cliquez ici pour en savoir davantage.**
Daily Validation Report (Rapport de validation journalier)	DVR	**Cliquez ici pour en savoir davantage.**
Payment Controls Service (Service de contrôles des paiements)	PCS	**Cliquez ici pour en savoir davantage.**
Shared Infrastructure Programme (Programme de partage d'infrastructures)	SIP	**Cliquez ici pour en savoir davantage.**
Business Identifier Code (code d'identification des banques)	BIC	**Cliquez ici pour en savoir davantage.**
Responsable de la sécurité des systèmes d'information	RSSI	Dénomination courante utilisée pour désigner le responsable du niveau hiérarchique le plus élevé redevable de la sécurité des systèmes d'information dans une entreprise

À propos de SWIFT

SWIFT est une coopérative mondiale appartenant à ses membres et le premier prestataire mondial de services de messagerie financière sécurisée. Nous fournissons à notre communauté une plateforme de messagerie et des normes de communication, et nous proposons des produits et services qui facilitent l'accès et l'intégration, l'identification, l'analyse et la conformité en matière de crime financier.

Notre plateforme de messagerie, nos produits et nos services connectent plus de 11 000 organisations bancaires et de titres, infrastructures de marché et entreprises clientes dans plus de 200 pays et territoires, leur permettant de communiquer en toute sécurité et d'échanger des messages financiers normalisés d'une manière fiable.

En tant que prestataire de confiance, nous facilitons les flux financiers mondiaux et locaux, apportons un soutien aux échanges et au commerce dans le monde entier ; nous visons constamment l'excellence opérationnelle et nous recherchons toujours de nouvelles manières de diminuer les coûts, limiter les risques et éliminer les inefficacités opérationnelles.

Ayant son siège social en Belgique, la gouvernance et la supervision internationale de SWIFT renforcent le caractère neutre et international de sa structure de coopérative. Le réseau mondial des bureaux de SWIFT assure une présence active dans tous les principaux centres financiers.

Pour en savoir davantage,
veuillez consulter le site
www.swift.com ou
contacter votre responsable de compte ou
envoyer un courriel à weareswift@swift.com.

57386 – Janvier 2019