Grant Thornton

Business Risk Services

Audit de conformité au *Customer Security Program* SWIFT.

Juillet 2022

SWIFT Customer Security Program

SWIFT fournit un réseau qui permet aux différentes institutions financières du monde entier d'envoyer et de recevoir des informations relatives aux transactions financières de manière sécurisée, standardisée et fiable.

SWIFT a défini un programme de sécurisation (CSP) qui vise à relever le niveau de sécurité des différents utilisateurs du réseau SWIFTnet afin de préserver sa sécurité.

Lancé en 2016 en réponse aux cyberattaques sophistiquées menées à l'encontre des utilisateurs de SWIFT, le programme de sécurité client (CSP) vise à :

- « élever la barre » de manière pragmatique en matière d'hygiène de cybersécurité pour tous les utilisateurs,
- réduire le risque de cyberattaques,
- minimiser l'impact financier d'opérations frauduleuses.

Depuis 2016, les utilisateurs de SWIFT étant confrontés à des attaques de plus en plus élaborées, des évolutions continues ont été réalisées.

Le mode opératoire, les tactiques, techniques et procédures (TTP) ont progressé et changé à mesure que les institutions renforcent les mesures de sécurité.

La persistance de telles menaces souligne l'importance de rester vigilant et proactif sur le long terme. Alors que les utilisateurs sont responsables de la protection de leurs propres environnements et accès à SWIFT, le CSP a été introduit pour soutenir les clients et favoriser la collaboration à l'échelle de l'industrie dans la lutte contre la cyberfraude.

Le CSP établit un ensemble commun de contrôles de sécurité connu sous le nom de *Customer Security Controls Framework* (CSCF) conçu pour aider les clients à sécuriser les environnements locaux et à favoriser un écosystème financier plus sûr.

Le *framework* CSCF de SWIFT

Le SWIFT CSCF comprend des **contrôles de sécurité obligatoires et optionnels** basés sur des standard de l'industrie, tels que NIST, ISO 27000 et PCI-DSS. Les contrôles de sécurité obligatoires établissent une ligne de base de sécurité pour l'ensemble de la communauté et doivent être mis en œuvre par tous les utilisateurs sur l'infrastructure SWIFT locale.

SWIFT donne la priorité aux contrôles obligatoires pour fixer un objectif réaliste de gains de sécurité tangibles à court terme, ainsi que de réduction des risques. Les contrôles optionnels sont basés sur les meilleures pratiques que SWIFT recommande aux utilisateurs de mettre en œuvre. Au fil du temps, les contrôles obligatoires peuvent évoluer en fonction du paysage des menaces, et certains contrôles optionnels peuvent devenir obligatoires.

SWIFT détaille tous les contrôles autour des trois objectifs généraux suivants :

Sécuriser son environnement

- Restreindre les accès Internet,
- Protéger les systèmes critiques du reste du SI,
- Réduire la surface d'attaque et les vulnérabilités,
- Sécuriser physiquement l'environnement.

Connaître et limiter l'accès

- Prévenir la compromission d'identifiant de connexion,
- Gérer les identités numériques et la séparation des privilèges.

Détecter et réagir

- Détecter les activités anormales au sein des systèmes et les transactions frauduleuses,
- Planifier la réponse à incident et le partage de connaissance.

Les contrôles ont été développés sur la base de l'analyse de SWIFT de l'état de la menace *cyber* actuelle et des avis d'experts du secteur ainsi que les commentaires des utilisateurs. Les contrôles sont également alignés sur les normes existantes de l'industrie de la sécurité de l'information.

L’évaluation de conformité au CSCF SWIFT obligatoire chaque année doit être réalisée par une équipe indépendante

Pour soutenir l'adoption des contrôles de sécurité, SWIFT a développé un processus qui demande aux utilisateurs **d'attester la conformité aux contrôles de sécurité obligatoires (et optionnels)** et de soumettre une attestation dans l'application KYC *Security Attestation* (KYC-SA).

À la fin de chaque année, **les utilisateurs doivent attester de la conformité aux contrôles de sécurité obligatoires (et facultatifs)** tels que documentés dans le CSCF en vigueur à ce moment-là. Généralement, une nouvelle version du CSCF est publiée en juillet, répertoriant les contrôles obligatoires et optionnels dont les utilisateurs doivent attester (à partir de juillet de l'année suivante lorsqu'ils sont mis en œuvre dans le KYC-SA). Autrement dit, les utilisateurs doivent attester **entre juillet 2022 et décembre 2022 des contrôles de sécurité répertoriés dans le CSCF v2022 publié à la mi-2021.**

Depuis 2021, **l’évaluation de la conformité au *framework* CSCF doit être effectuée par une équipe indépendante**. Pour faciliter davantage ces évaluations, SWIFT rappelle aux utilisateurs :

- Que le respect des objectifs de contrôle est une approche basée sur les risques. Les directives de mise en œuvre fournies peuvent être utilisées comme point de départ, mais ne peuvent pas être considérées comme des listes de contrôle d'audit strictes.

- Que les utilisateurs s'engageant avec des tiers (y compris des fournisseurs de *cloud*) pour héberger ou exploiter (en totalité ou en partie) leur propre infrastructure SWIFT doivent obtenir une assurance raisonnable que les activités externalisées ou les composants hébergés en externe sont protégés par les contrôles de sécurité.

Les tiers peuvent s'appuyer sur leur programme de conformité, qui se base généralement sur les certifications ou l'assurance SOC 2, PCI-DSS ou NIST pour répondre aux utilisateurs qui interagissent avec eux et cartographier les contrôles de sécurité du CSCF.

Intégration à la gouvernance de la sécurité et la gestion des risques

SWIFT encourage les utilisateurs à considérer la gestion des risques cyber dans les termes les plus larges possibles, y compris au-delà de la portée de l'infrastructure SWIFT de l'utilisateur et des contrôles de sécurité SWIFT. Pour une gestion plus efficace, les utilisateurs ne doivent pas envisager la mise en œuvre de ces contrôles de sécurité comme une activité ni ponctuelle, ni comme exhaustive ou globale.

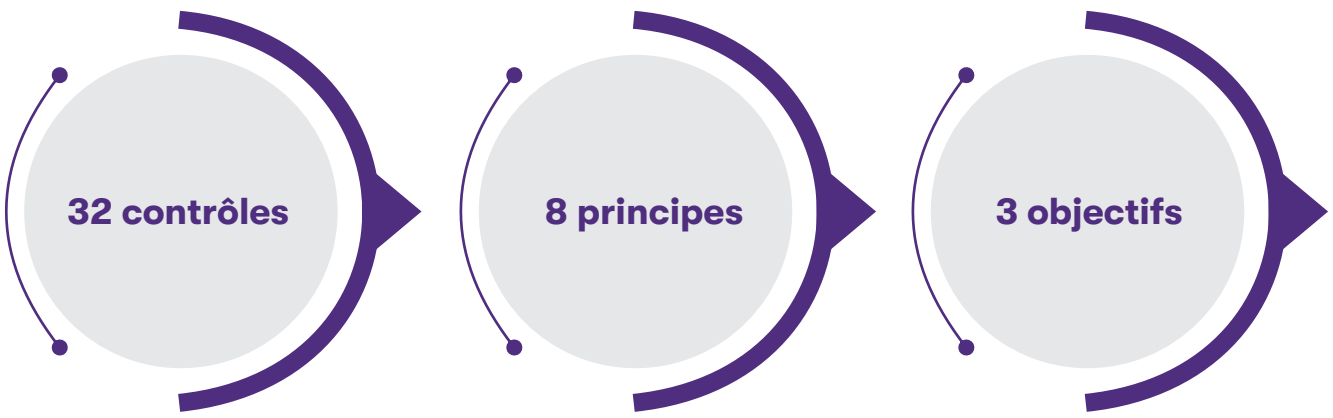
Les utilisateurs doivent plutôt intégrer les contrôles de SWIFT dans un programme continu de gouvernance et de gestion des risques de cybersécurité au sein de leur organisation, en tenant compte d'un bon jugement et des meilleures pratiques les plus récentes d'une part, et en tenant compte de l'infrastructure et des configurations spécifiques à l'utilisateur d'autre part. En conséquence, les utilisateurs peuvent réutiliser et bénéficier des politiques, procédures et contrôles existants qui ont été établis pour gérer d'autres domaines de cyber-risques.

Une approche holistique du cyber-risque est la plus efficace, améliorant ainsi la sécurité globale de chaque organisation individuelle et de la communauté financière au sens large.

De plus, les utilisateurs doivent avoir le niveau correct de responsabilité et de surveillance pour leurs activités de gestion des cyber-risques. Généralement, le responsable de la sécurité de l'information joue un rôle de premier plan dans ce domaine en dirigeant les priorités du programme de sécurité et en sollicitant le soutien et les conseils appropriés du conseil d'administration.

Objectifs, principes et contrôles

SWIFT décrit les objectifs, les principes et les contrôles constituant son *framework* d'évaluation CSCF comme suit :



Les contrôles de sécurité sont basés sur trois objectifs généraux, soutenus par huit principes de sécurité. Les objectifs constituent la structure de niveau le plus élevé pour la sécurité dans l'environnement local de l'utilisateur.

Les principes associés précisent les domaines d'intervention les plus prioritaires au sein de chaque objectif.

Les 32 contrôles de sécurité (23 contrôles obligatoires et 9 contrôles optionnels) détaillés dans le *framework* CSCF sous-tendent ces objectifs et ces principes. Les contrôles permettent d'atténuer les risques de cybersécurité spécifiques auxquels les utilisateurs de SWIFT sont confrontés.

Dans chaque contrôle de sécurité, SWIFT a documenté les facteurs de risque les plus courants pour lesquels le contrôle est conçu afin de les atténuer.

La gestion de ces risques vise à prévenir ou à minimiser les conséquences commerciales indésirables et potentiellement frauduleuses, telles que :

- L'envoi ou la modification non autorisés de transactions financières,
- Le traitement des transactions entrantes SWIFT modifiées ou non autorisées (c'est-à-dire les transactions reçues),
- Les affaires menées avec une contrepartie non autorisée,
- La violation de la confidentialité (des données commerciales, des systèmes informatiques ou des détails de l'opérateur),
- L'atteinte à l'intégrité (des données commerciales, des systèmes informatiques ou des détails de l'opérateur).

En fin de compte, ces conséquences représentent des risques multiples pour l'entreprise :

- Risques financiers,
- Risques juridiques,
- Risques réglementaires,
- Risques réputationnels.

Grant Thornton

Grant Thornton est en première ligne pour assister les entreprises à évaluer leur niveau de conformité aux exigences de sécurité SWIFT.

Son expertise en gestion du risque *cyber* et son expérience quant à l'évaluation de la sécurité du système d'information de ses clients permet à Grant Thornton d'être référencé auprès de SWIFT comme évaluateur indépendant et accrédité pour la zone Europe. La cabinet aide ainsi les entreprises quel que soit leur de toute taille à identifier les écarts potentiels qu'elles possèderaient avec les exigences du *framework* CSCF.

Les équipes de Grant Thornton sauront définir le programme d'audit adéquat et adapté à chaque cas de figure, afin d'identifier les points de contrôle portés par les équipes du client et ceux qui doivent être couverts par des tiers impliqués de manière plus ou moins importante dans les interactions avec le réseau SWIFTnet (ie. fournisseur *cloud* de plateforme de trésorerie, service bureau SWIFT, etc.).

Au-delà de l'évaluation des écarts avec les exigences *cyber* définies par SWIFT, les travaux menés par les équipes permettront d'alimenter la feuille de route sécurité de l'entreprise.

Découvrez nos activités en cliquant ici.

210 M€
chiffre d'affaires

23
bureaux

2 000
collaborateurs

125
associés

5,4% de croissance en 2021

86 sociétés cotées auditées dont **environ 50** **« *small&mid cap* »**

122 Entités d'Intérêt Public auditées *

75% des Groupes du CAC 40 accompagnés

Nicolas GUILLAUME

Associé,
en charge de l'offre *Business Risk Services*

Coordonnées :
+33 6 11 12 52 16

nicolas.guillaume@fr.gt.com

www.grantthornton.fr

Grant Thornton France

@GrantThorntonFr

Grant Thornton France