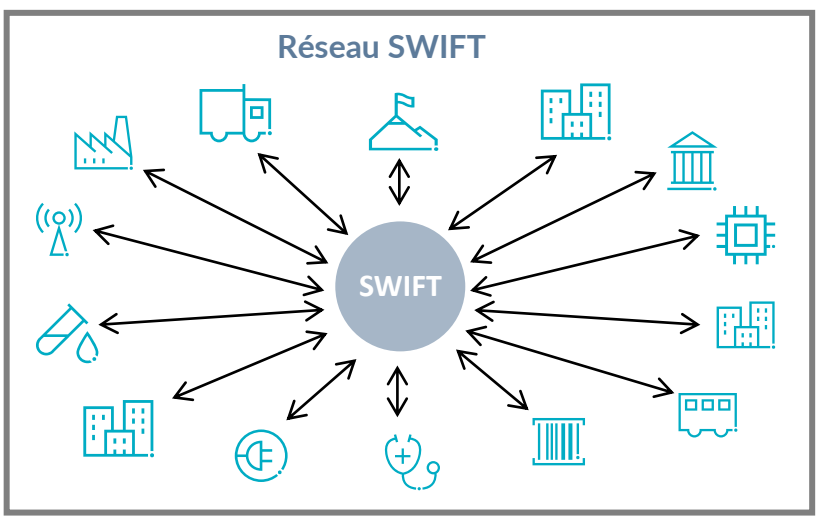
protiviti®
Global Business Consulting

SWIFT – Customer Security Program – CSCF 2024

SWIFT, fournisseur mondial de services de messagerie financière, connecte plus de 11 000 institutions financières et grandes entreprises de différents secteurs d'activité dans le monde. Utilisant les différents types de formats de messages et de protocoles financiers à disposition, les clients membres de SWIFT s'échangent quotidiennement plus de 40 millions de messages pour des transactions financières ou ordre de paiements.

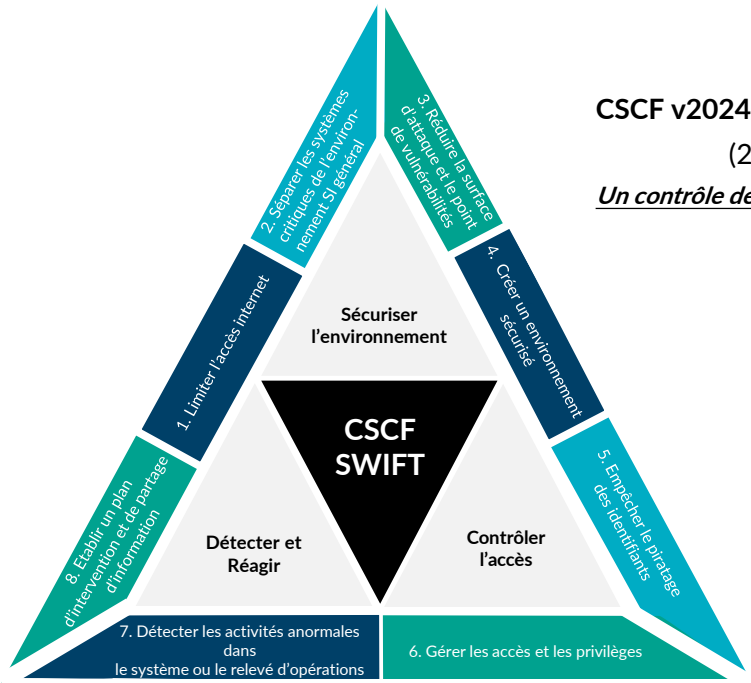


En réponse à l'augmentation des fraudes financières et des cyberattaques qui deviennent de plus en plus sophistiquées et globales, SWIFT a défini dès 2017 un programme de sécurité, le « **Customer Security Program** » (**CSP**). Il repose sur un référentiel de contrôles, le « **Customer Security Controls Framework**" (**CSCF**). Ce référentiel est évolutif, s'impose aux membres et sa mise en œuvre doit faire l'objet depuis 2021 d'une évaluation indépendante annuelle qui sert de base à l'attestation de sécurité qui leur est demandée. Chaque membre SWIFT se doit donc de déployer les mesures de sécurité préconisées et d'être à même d'en rendre compte en vue de renforcer la protection du réseau SWIFT auquel il est connecté et de ses membres.

L'approche et le périmètre de l'évaluation dépendent du type d'architecture SWIFT en place au sein du système d'information du client SWIFT, il en existe cinq; A1, A2, A3, A4 et B.

Qu'est-ce que le référentiel de contrôles (CSCF) ?

Il s'agit d'un ensemble de 32 contrôles de sécurité - obligatoires (25) et optionnels (7) - structuré par objectif et requis pour renforcer la prévention et la détection de l'utilisation frauduleuse des infrastructures SWIFT gérées par les clients. Ils servent de base aux travaux de l'évaluation indépendante de sécurité SWIFT et à l'**attestation de sécurité obligatoire KYC-SA** (Know Your Customer- Security Attestation) à établir par le client SWIFT.



CSCF v2024 : 3 objectifs, 7 principes et 32 contrôles

(25 obligatoires et 7 facultatifs)

***Un contrôle devient obligatoire en 2024** : le 2.8* **« Outsourced Critical Activity Protection »**

Evolution de l'attestation annuelle SWIFT

Les contrôles obligatoires exigés par SWIFT sont enrichis au fil des années en réponse aux nouvelles menaces de cybersécurité.

2017-2020

Attestation annuelle sur base d'auto-évaluation (27 contrôles)

2021

Attestation établie pour la première fois sur la base d'une évaluation indépendante obligatoire (interne ou externe) selon CSCF v2021 (31 contrôles)

2022-2023

Attestation établie sur la base d'une évaluation indépendante obligatoire (interne ou externe)

2024

Attestation établie sur base d'une évaluation indépendante obligatoire (interne ou externe) selon le CSCF v2024 (32 contrôles – 25 obligatoires)

Quelles sont les principales nouveautés pour 2024 ?

- Le contrôle **« 2.8 Outsourced Critical Activity Protection »** est désormais obligatoire pour toutes les architectures.
- De nouvelles précisions sont apportées sur les typologies des **« Outsourcing agents »** proposant des services d'hébergement et de gestion de l'infrastructure SWIFT ou bien la fourniture de services d'accès au réseau SWIFT (service bureau (SB), Business Connect (BC) ou Lite2 Business Application (L2BA) provider).

Qui doit réaliser l'évaluation indépendante ?

- Les clients SWIFT sont libres de choisir des ressources internes ou externes à leur organisation pour réaliser cette évaluation dès lors qu'elles sont indépendantes, compétentes et certifiées.

  - ✓ **Dans le cas de l'utilisation de ressources internes**, l'équipe d'évaluation doit être indépendante de la 1ère ligne de défense (RSSI) : les équipes éligibles sont généralement l'Audit Interne (3ème ligne de défense), le Risk Manager ou la Direction Conformité (2ème ligne de défense) ou encore une équipe indépendante spécifiquement mise en place pour l'évaluation. Elle doit posséder une expérience réelle en évaluation de la cybersécurité selon les normes de l'industrie (ex ISO 27001, NIST CSF, PCI DSS, etc.) et détenir au moins une certification professionnelle pertinente.

  - ✓ **Dans le cas d'utilisation de ressources externes (comme Protiviti),** le prestataire sélectionné doit posséder une expérience réelle en matière d'évaluation de la cybersécurité selon les normes de l'industrie telles que ISO 27001, NIST CSF ou PCI DSS et il doit détenir au moins une certification professionnelle pertinente en sécurité des systèmes d'information.

NB: SWIFT peut également demander directement à ses clients une évaluation indépendante qui dans ce cas sera nécessairement réalisée par des ressources externes.

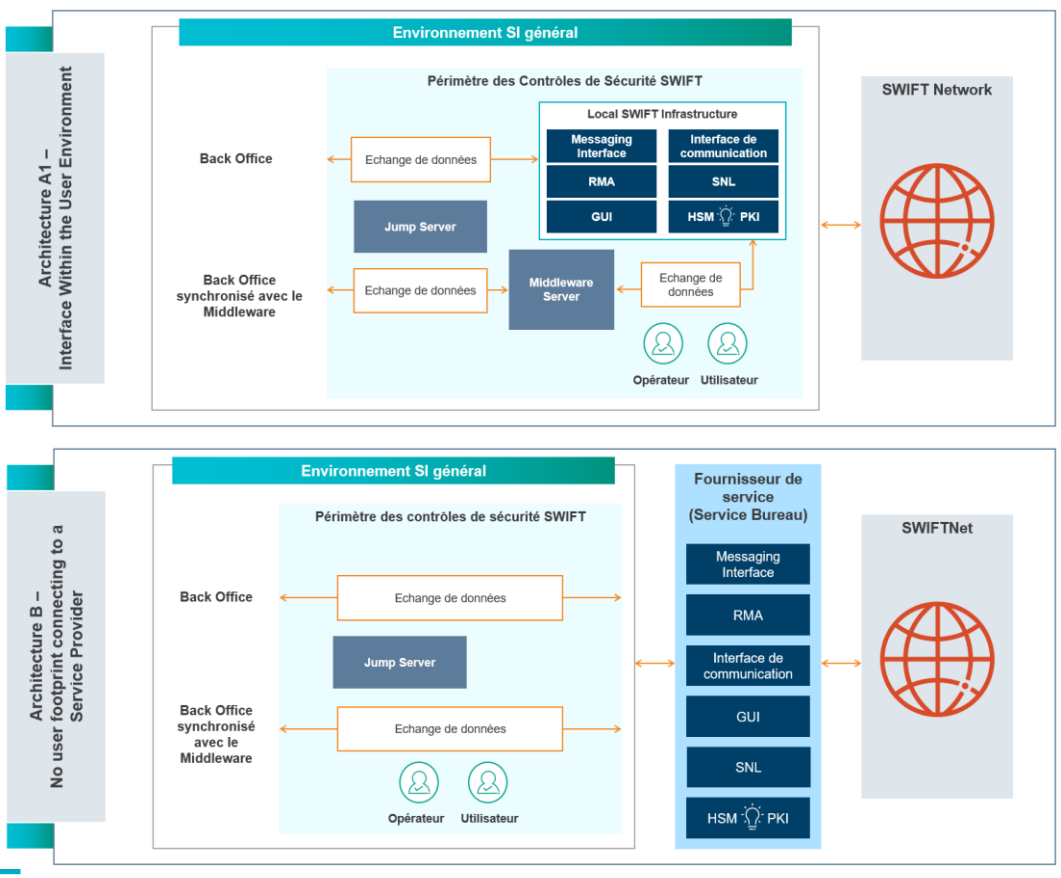
Quel périmètre pour l'évaluation indépendante ? Une démarche spécifique à chaque architecture SWIFT en place chez le client.

Pour être en conformité avec le CSCF v2024, le client se doit d'évaluer son environnement SWIFT et certains des composants de son SI pouvant impacter sa sécurité. On comprend ainsi que le périmètre de revue dépend fortement de l'architecture (A1, A2, A3, A4 ou B) spécifique mise en place par le client.

Les architectures SWIFT de types **A1** et **B présentées** ci-dessous à titre d'exemples mettent ainsi en évidence la différence de périmètre à considérer pour l'évaluation en fonction des composants SWIFT hébergés dans l'environnement du client (interne ou cloud).

Architecture SWIFT A1 & B :

L'architecture A1 qui compte plus de composants SWIFT hébergées chez le client expose ce dernier à des risques accrus en termes de sécurité, confidentialité et intégrité des données et en conséquence le périmètre des contrôles à évaluer est plus large sur l'architecture A1 que sur l'architecture B.



Ajoutons qu'en tout état de cause, il sera tenu compte pour la définition du périmètre de l'évaluation CSP 2024 du rapport de l'évaluation indépendante réalisée en 2023 ainsi que des changements réalisés sur l'environnement SWIFT en production, le cas échéant.

Comment appréhender l'évaluation 2024 : nouvelle évaluation indépendante complète ou simple évaluation « delta » SWIFT CSCF ?

Faut-il chaque année reproduire les travaux ou peut-on s'appuyer sur une évaluation indépendante antérieure?
La réutilisation des conclusions d'une évaluation SWIFT CSP n'est en tout état de cause possible que si la date de fin de la précédente évaluation est antérieure de moins de deux (2) ans. En outre, les éventuelles faiblesses identifiées lors de l'évaluation et ayant un impact sur la conformité à un objectif de contrôle doivent avoir été corrigées par l'entreprise. Une vérification de leur traitement doit être effectuée par une partie indépendante; il peut s'agir d'un évaluateur interne ou externe. Il n'est pas nécessaire que ce soit le même intervenant/prestataire que celui a soulevé l'observation originale.

Par ailleurs, il convient de distinguer trois cas distincts, comme présenté ci-dessous :

Cas 1:
Nouvelle évaluation N+1 SWIFT CSCF complète non requise si les conditions 1, 2 et/ou 3 ci-dessous sont réunies:

1. L'évaluateur confirme la validité de l'évaluation indépendante réalisée en N.
2. L'environnement client en cours d'évaluation n'a pas subi de changements significatifs* qui invalideraient les conclusions de l'évaluation complète en N+1.
3. Le nouveau CSCF n'inclut pas de nouveaux contrôles obligatoires ou des changements aux contrôles qui ne sont pas couverts par l'évaluation.

Cas 2:
Évaluation delta SWIFT CSCF suffisante si les conditions 2 et/ou 3 ne sont pas applicables.**

Cas 3:
Nouvelle Evaluation SWIFT CSCF requise si les conditions 1, 2 et/ou 3 ne sont pas réunies.

Evaluation SWIFT CSCF Complète Obligatoire
Mandatée par SWIFT ou Indépendante
(Externe ou Interne)

Evaluation SWIFT CSCF Complète Obligatoire
si aucune delta/nouvelle évaluation faite en N+1 (au contôle près)
Mandatée par SWIFT ou Indépendante
(Externe / Interne)

(*) Les changements significatifs qui pourraient empêcher la réutilisation d'une évaluation SWIFT antérieure sont par exemple : la migration vers un nouveau système d'exploitation (de Linux à Windows), les changements de version majeure de l'interface de messagerie ou de communication, l'ajout de matériel dans les composants du champ d'application, les changements dans la connectivité réseau du client (par exemple, de la connectivité du bureau de service à Lite 2).

(**) Évaluation Delta : L'évaluation delta ne couvre que les changements MINEURS apportés aux composants couverts par l'audit ou aux contrôles qui ont été modifiés ou ajoutés depuis le dernier audit.

L'approche de Protiviti pour réaliser l'évaluation indépendante CSCF SWIFT 2024

Réaliser une évaluation selon le cadre de contrôles CSCF **Customer Security Controls Framework** n'a pas pour objet d'auditer l'ensemble du système d'information du client, mais de vérifier l'existence des bonnes pratiques de sécurité sur le périmètre considéré.

Doivent être considérés en particulier l'architecture en place, la configuration des systèmes, l'isolement relatif des environnements SWIFT en interne.

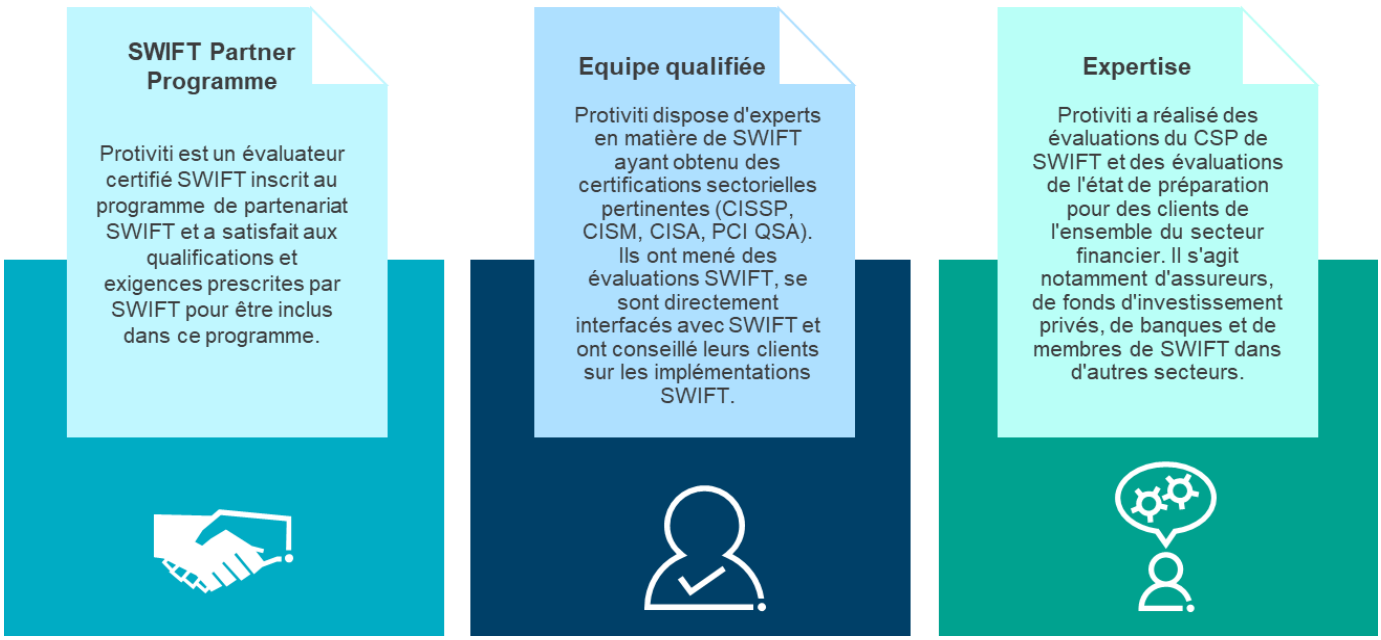
L'approche de travail que nous avons développé chez **Protiviti** prend en compte ces différents éléments.

Les étapes de notre approche pour l'évaluation CSCF SWIFT

- ***Identifier / valider le type l'architecture SWIFT*** *en place et définir le périmètre des contrôles.*
- ***Prendre en compte le cas échéant les rapports des évaluations indépendantes*** *des années précédentes (moins de 2 ans).*
- *Identifier les* ***éventuels changements*** *ayant impacté l'environnement de production SWIFT et ainsi potentiellement les conclusions des évaluations indépendantes précédentes.*
- ***Réaliser les contrôles obligatoires*** *et optionnellement les contrôles additionnels recommandés par SWIFT.*
- *Analyser les réponses aux questionnaires ainsi que les éléments probants collectés et* ***évaluer les risques*** *éventuellement identifiés.*
- *Proposer un* ***plan de remédiation*** *des vulnérabilités identifiées.*
- *Assister les clients dans la* ***mise en place des recommandations*** *proposées afin de pallier aux vulnérabilités identifiées.*
- *Réaliser une* ***veille continue*** *pour surveiller l'état de conformité.*

Pourquoi Protiviti pour vous accompagner dans la démarche de conformité ?

- Protiviti est un cabinet de conseil référencé par SWIFT pour délivrer des missions d'évaluation selon le cadre CSCF du CSP.
- Les équipes Protiviti ont une large expérience de la réalisation de missions d'audit des environnements SWIFT dans des architectures hétérogènes et plus largement de la sécurité des systèmes d'information dans une multitude de secteurs.
- Les consultants Protiviti disposent de plusieurs certifications dans les domaines de l'audit SI, de la sécurité SI, de l'organisation des systèmes d'information et des infrastructures SI.



Contacts

Bernard Drui
Managing Director & Country Market Lead
Bernard.Drui@protiviti.fr

Anis Hammami
Associate Director – SWIFT Expert
Anis.Hammami@protiviti.fr