

SWIFT CUSTOMER SECURITY PROGRAM (CSP)



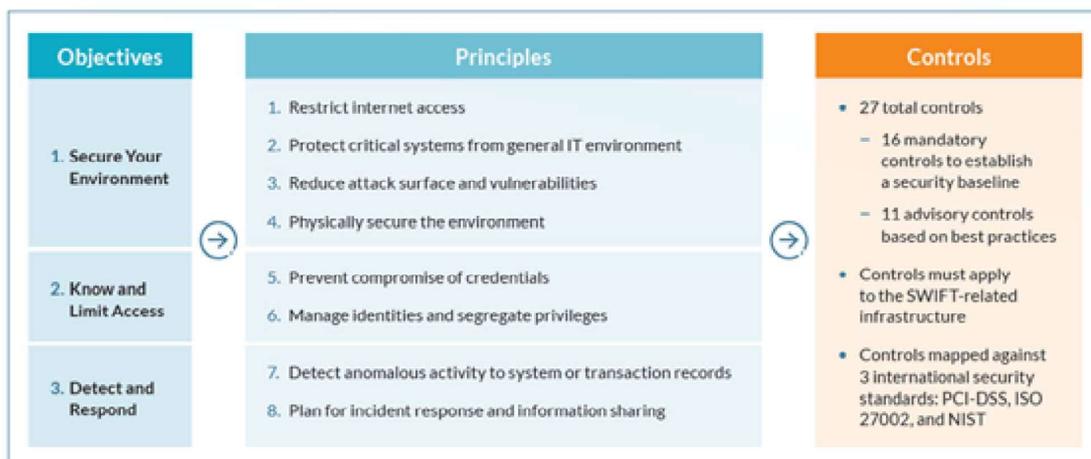
Qu'est-ce que SWIFT CUSTOMER SECURITY PROGRAM (CSP)?

SWIFT a lancé sa plateforme de contrôle **CSCF** afin d'optimiser la transparence et l'intégrité au sein de son réseau financier. Le programme CSP de SWIFT est axé sur 3 domaines :

- Protéger et sécuriser votre environnement local
- Prévenir et détecter les fraudes au sein de votre réseau commercial
- Se préparer à répondre aux futures cyberattaques

Pendant que la plupart des clients sont axés sur la protection de leur environnement, SWIFT CSP a pour but de protéger son réseau dans la lutte contre les cybers attaques.

- • • **SWIFT Customer Security Controls Framework (CSCF)**



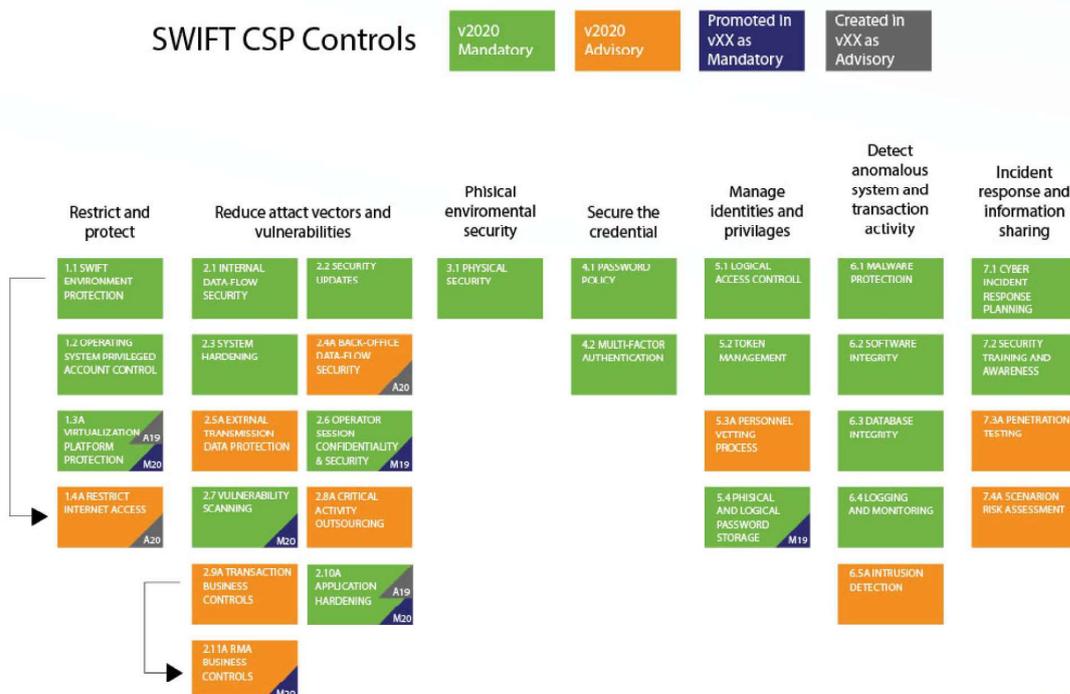
Pourquoi est-il important d'appliquer le programme CSP ?

En réponse à plusieurs attaques et brèches durant l'année 2016, SWIFT a identifié en 2017, 16 contrôles de sécurité obligatoires et 11 contrôles de sécurité optionnels pour tous ses 11.000 clients à travers le monde. Ainsi tous les clients du réseau SWIFT doivent certifier et attester qu'ils sont en règle et ont bel et bien implémenté ces contrôles tout en partageant ces résultats avec les autres parties et les régulateurs.

Comment cela impacte-t-il les clients ?

Le **SWIFT CSCF** a évolué depuis l'implémentation du **CSP**. Les clients continueront à implémenter les contrôles de sécurité et à augmenter leur niveau de conformité vis-à-vis du **CSCF**. Aujourd'hui en 2020, les clients **SWIFT** doivent attester qu'ils sont conformes au **CSCF**. La mise à jour de cette plateforme contient 19 contrôles de sécurité obligatoires et 10 optionnels.

Depuis 2020, **SWIFT** a donné un statut obligatoire à 2 contrôles existant qui autrefois étaient optionnels et a introduit 2 contrôles optionnels additionnels parmi les 21 obligatoires et les 10 optionnels au sein de la plateforme **CSCF v2020**. En plus de l'ajout de 2020, tous les clients SWIFT devraient subir une évaluation indépendante en plus de l'auto-évaluation afin d'être conforme au **SWIFT CSCF**.



Comment CYBERIX peut vous aider ?

Notre équipe d'experts travaille depuis des années dans les secteurs du transfert d'argent et des paiements, de la sécurité, de la gestion des risques et de la conformité. Ce savoir-faire acquis durant de longues années a enrichi notre professionnalisme et fait de nous un partenaire idéal dans la réalisation des évaluations de risque et des audits en environnement **SWIFT**. Nous vous accompagnerons de façon efficace dans la conception et l'implémentation des contrôles qui permettront de fermer toute brèche avec le **SWIFT SCP** et de vous aligner aux normes internationales telles que **PCI-DSS**, **ISO27002**, **NIST**. Nous vous assisterons dans la planification et la réalisation de votre attestation **SWIFT CSP** et de la conformité à **SWIFT CSCF**.

Nos services

- Tests de pénétration en environnement SWIFT
- Formation à la sensibilisation cyber sécuritaire
- Évaluation des risques et étude des vulnérabilités
- Nous vous assisterons et vous accompagnerons tout au long du processus d'implémentation de SWIFT CSP en vous fournissant une approche sur mesure. Nos professionnels dans les métiers de la cyber-sécurité sont tous certifiés et très familiers de l'industrie bancaire.

Nous contacter



SIEBADJI Emmanuel
Security Analyst, Auditor
+237 673 41 60 22
s.emmanuel@cyberix.fr



TALOM Michel
Network Engineer, Auditor
+237 699 95 79 76
michel.talom@cyberix.fr



KUATE Gael
Forensic investigator, Auditor
+237 690 57 21 96
gael.kuate@cyberix.fr



FOUMAKOUNDI Joseph
Data Recovery, Auditor
+237 696 53 07 17
f.tata@cyberix.fr



 (+237) 696 04 28 43 / 650 46 21 72

 B.P. 10001 / Douala

 www.cyberix.fr

 cspswift@cyberix.fr