



www.citizecan.fr



SWIFT – Customer Security Program 2022

Présentation
générale

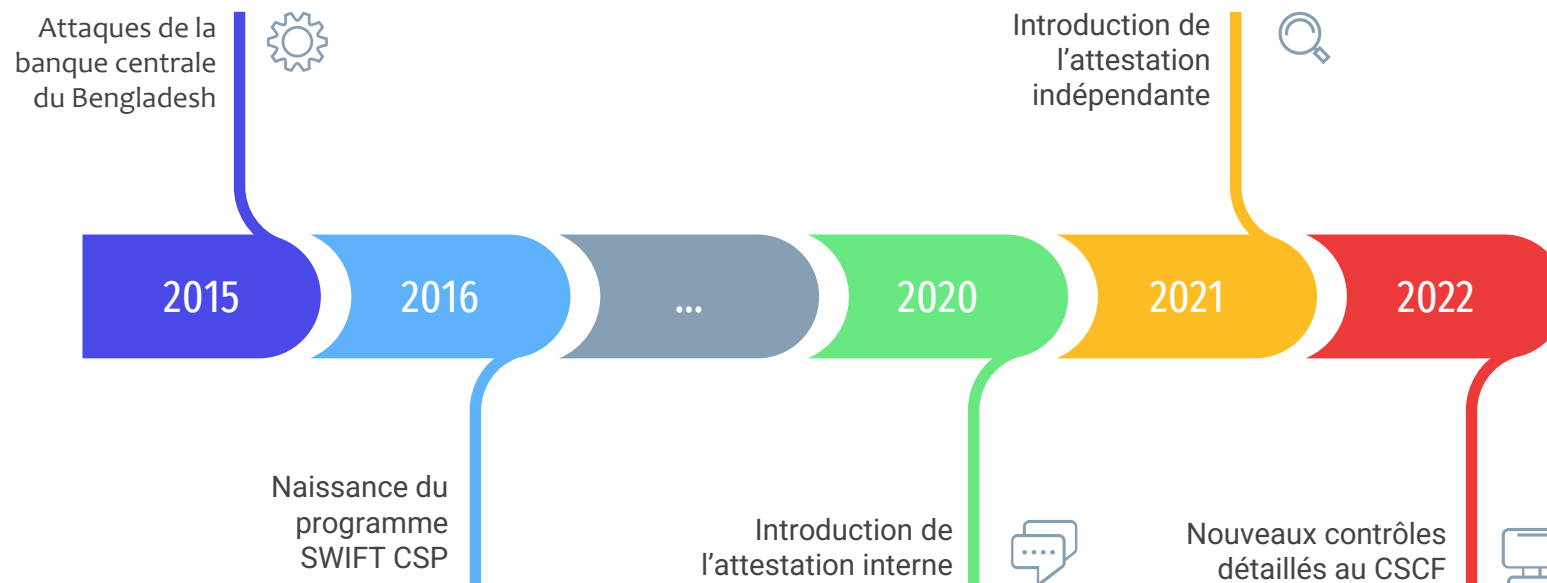
SWIFT CSP - Chronologie

En réponse aux attaques perpétrées en février 2016 (Banque centrale du Bangladesh - 81 millions de dollars), SWIFT a lancé en 2016 le programme de sécurité client (**CSP - Customer Security Program**).

Depuis l'année 2021, SWIFT a introduit la nécessité d'étayer l'attestation par une évaluation indépendante (évaluation et non un audit complet).

La nouvelle version du CSCF 2022 a été publiée au début du mois de juillet 2021 et recense les mesures obligatoires et conseillées pour les attestations (déclaration à partir du mois de juillet 2022 lors de l'ouverture de la campagne dans l'application KYC-SA).

Les clients SWIFT doivent se conformer au SWIFT CSCF v2022 défini en juillet 2021, au plus tard le 31 décembre 2022.



SWIFT CSP - Périmètre

23 contrôles
obligatoires

9 contrôles
facultatifs

1 contrôle
rendu
obligatoire
en 2022

Sécuriser et protéger

Définition d'un cadre de contrôles de sécurité. Le Customer Security Controls Framework (CSCF) décrit un ensemble de règles et contrôles obligatoires ou facultatifs qui doivent être mis en œuvre annuellement par tous les utilisateurs sur leur infrastructure SWIFT.

Déclaration dans le portail SWIFT

Déclaration annuelle de son niveau de conformité aux contrôles entre juillet et le 31 décembre.

Utilisation de l'application KYC Security Attestation (KYC-SA) sur le site internet de SWIFT. Double signature interne, accompagnée de l'attestation indépendante.

Customer Security Controls Framework 2022

Des contrôles existants voient désormais leur périmètre étendu. C'est le cas du contrôle « 1.2 » à propos de la gestion des comptes privilégiés.

Périmètre du CSP SWIFT

Toutes les architectures utilisant un composant connecté au réseau SWIFT sont considérées dans le cadre du CSP SWIFT. Une typologie précise a été définie (A1 > ... > B) permettant de définir des contrôles adéquats pour toutes les organisations.

A travers ce programme, SWIFT entend renforcer le niveau de sécurité de son réseau et sensibiliser les parties prenantes aux risques liés à la cybersécurité.

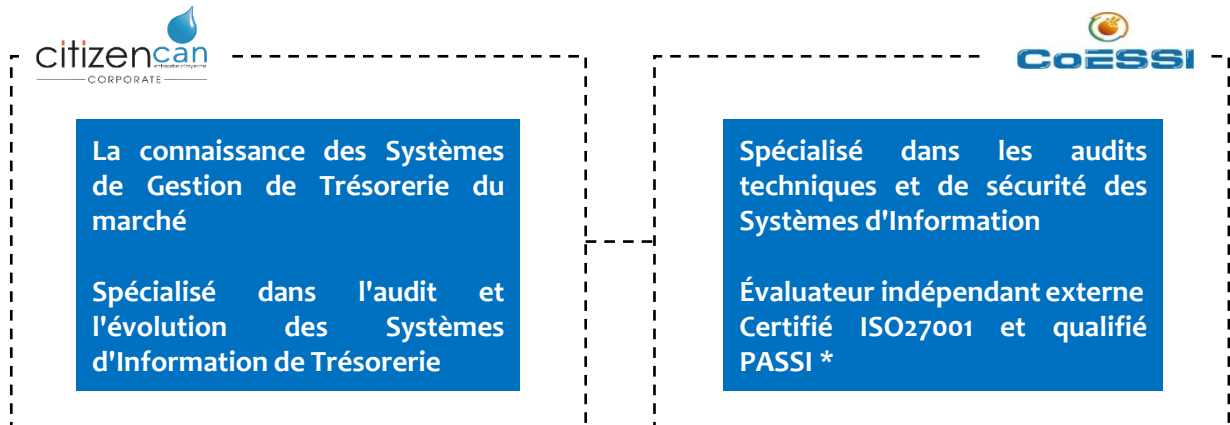
SWIFT procède à une analyse des attestations, par échantillon, et peut également mandater un audit en propre.

SWIFT CSP – Notre accompagnement

Citizen Can Corporate, en partenariat avec CoESSI, prend en charge les besoins de certification SWIFT du Customer Security Program (CSP).

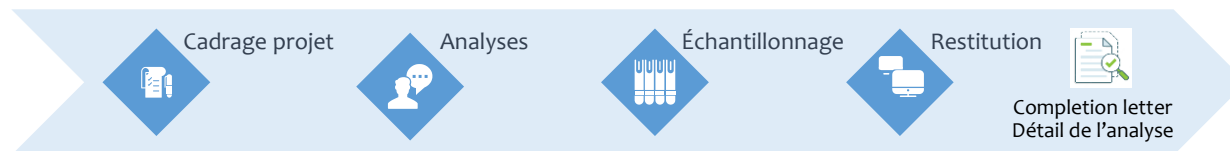
Nous couvrons les besoins détaillés dans le CSCF 2022 (Customer Security Controls Framework) et au-delà.

Nous sommes évaluateur indépendant qualifié (PASSI-RGS*), également apte à prendre en charge les futurs contrôles obligatoires demandés par SWIFT (tests d'intrusion, contrôle des comptes système etc.)



Notre accompagnement

- Une approche éprouvée
- Une démarche de certification (éléments de preuve à fournir)
- Certification des mesures liées aux contrôles obligatoires listés dans le CSCF (analyse des forces de preuve et échantillonnage)
- Livrables : Customer Completion Letter, note de synthèse détaillant l'analyse fonctionnelle et technique réalisée



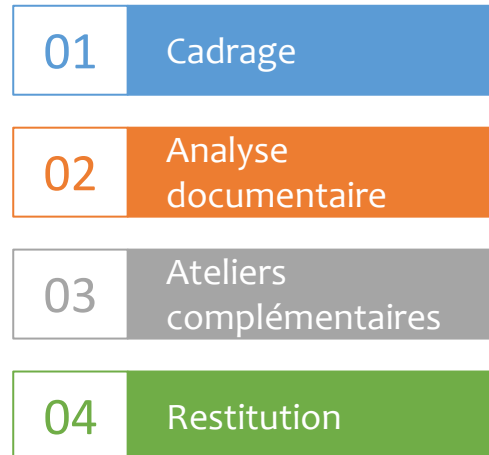
- Au-delà du périmètre CSP SWIFT, nous pouvons également intervenir sur des missions de gestion des enjeux de cybersécurité : formation, tests d'intrusion, tests de phishing, audit de vulnérabilité de l'infrastructure technique, définition de procédure de réponse à incident de cybersécurité, analyse des risques contractuels etc.

* La qualification des prestataires d'audit de la sécurité PASSI fait partie du règlement général de sécurité (RGS) de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

CSP SWIFT 2022

OFFRE FORFAITAIRE

- Approche standardisée, au forfait - checklist initiale et revue de l'existant intégrés à la mission
- Les honoraires prennent en compte l'ensemble des activités relatives à la certification définie par SWIFT dans le cadre du programme CSP 2022
- Livrables identifiés : Customer Completion Letter, note de synthèse détaillant l'analyse fonctionnelle et technique réalisée



Certification proposée en forfait

- Audit fonctionnel et technique du programme CSP SWIFT 2022
- Production des livrables documentaires
- Pilotage de la mission, gouvernance simplifiée

Liste des contrôles détaillés au CSCF

MISE À JOUR 2022 – EXTRACT FROM SWIFT

Mandatory and Advisory Security Controls	Architecture Type				
	A1	A2	A3	A4	B
1 Restrict Internet Access and Protect Critical Systems from General IT Environment					
1.1 SWIFT Environment Protection	•	•	•		
1.2 Operating System Privileged Account Control	•	•	•	•	•
1.3 Virtualisation Platform Protection	•	•	•	•	
1.4 Restriction of Internet Access	•	•	•	•	•
1.5A Customer Environment Protection	○	○	○	•	
2 Reduce Attack Surface and Vulnerabilities					
2.1 Internal Data Flow Security	•	•	•		
2.2 Security Updates	•	•	•	•	•
2.3 System Hardening	•	•	•	•	•
2.4A Back Office Data Flow Security	•	•	•	•	•
2.5A External Transmission Data Protection	•	•	•	•	
2.6 Operator Session Confidentiality and Integrity	•	•	•	•	•
2.7 Vulnerability Scanning	•	•	•	•	•
2.8A Critical Activity Outsourcing	•	•	•	•	•
2.9 Transaction Business Controls	•	•	•	•	•
2.10 Application Hardening	•	•	•		
2.11A RMA Business Controls	•	•	•	•	•
3 Physically Secure the Environment					
3.1 Physical Security	•	•	•	•	•

4 Prevent Compromise of Credentials					
4.1 Password Policy	•	•	•	•	•
4.2 Multi-Factor Authentication	•	•	•	•	•
5 Manage Identities and Separate Privileges					
5.1 Logical Access Control	•	•	•	•	•
5.2 Token Management	•	•	•	•	•
5.3A Staff Screening Process	•	•	•	•	•
5.4 Physical and Logical Password Storage	•	•	•	•	•
6 Detect Anomalous Activity to Systems or Transaction Records					
6.1 Malware Protection	•	•	•	•	•
6.2 Software Integrity	•	•	•	•	
6.3 Database Integrity	•	•		•	
6.4 Logging and Monitoring	•	•	•	•	•
6.5A Intrusion Detection	•	•	•	•	
7 Plan for Incident Response and Information Sharing					
7.1 Cyber Incident Response Planning	•	•	•	•	•
7.2 Security Training and Awareness	•	•	•	•	•
7.3A Penetration Testing	•	•	•	•	•
7.4A Scenario Risk Assessment	•	•	•	•	•

Groupe Citizen Can

NOUS AIMONS NOTRE MÉTIER, NOUS SOUHAITONS LE PARTAGER

Les sociétés du GROUPE CITIZEN CAN conduisent et réalisent les projets d'évolution des organisations et systèmes d'informations des directions financières Corporate et bancaires.

Domaines d'intervention

- Paiements EDI bancaires
- Gestion de la trésorerie
- Opérations de Marché
- Gestion des risques (change, taux)
- Conformité, Comptabilité
- In House Banking

Les points clés

- Plus de 40 consultants métiers (trésoriers, éditeurs de logiciels financiers, société de conseil)
- Créateur de la Méthode citoyenne adaptée à vos projets.



Groupe
citizencan
entreprises citoyennes

citizencan
CORPORATE
entreprise citoyenne

Arc-en-Ciel
Consultants

citizencan
SPAIN



PLATINIUM Top 1%
2020
ecovadis
CSR
Rating

Citizen Can a obtenu le label PLATINIUM EcoVadis sur sa performance RSE (Responsabilité Sociétale des Entreprises)



Citizen Can s'engage pour la promotion de la Charte de la Diversité

Notre mission consiste à agir, en amont, sur la stratégie et l'organisation, et en aval, sur les Système d'Information et les processus de Trésorerie.

Groupe Citizen Can

NOUS AIMONS NOTRE MÉTIER, NOUS SOUHAITONS LE PARTAGER

Nos consultants possèdent les compétences et les qualités nécessaires au bon déroulement des projets

- Compétences métiers (comprendre les objectifs, proposer des solutions)
- Méthodes d'organisation (gérer les projets, respecter le planning)
- Communication (rédiger les spécifications, diriger les équipes, transférer des compétences)
- Respect des valeurs du Corporate (présentation, horaires, hiérarchie)
- Rigueur et discipline (clarté des livrables, organisation des actions)
- Charisme (facilité d'intégration, respecté et écouté)



CoESSI est une société de conseil spécialisée dans la sécurité des systèmes d'information. Elle met en œuvre un savoir-faire issu de plus de 20 ans d'expérience en Sécurité des Systèmes d'Information, qui lui apporte pertinence et efficacité dans ses missions

Son spectre d'activité s'étend du conseil stratégique et organisationnel (politique de sécurité, schéma directeur...) aux missions à fortes composantes technologiques (tests intrusifs, mise en place de PKI, SSO...)

- Conseil et Expertise
 - Assistance à MOA et MOE (rédaction de CCTP, dépouillement et analyse des offres, suivi et coordination de projet)
 - Études en architectures de sécurité (internet, nomades, gestion des identités [IAM], signature unique [SSO], infrastructure à clés publiques [PKI], tunnel chiffré [VPN], protection des données [DLP]...)
 - Assistance à la mise en place et à l'administration de solutions de sécurité
 - Délégation sur site de compétences d'expertise en sécurité
- Audits
 - Analyse de risques métiers et informatiques
 - Audits organisationnels de sécurité (audits généraux, audits des processus)
 - Évaluations de conformité (ISO 27XXX, diagnostics de contrôle interne, PCI-DSS...)
 - Audits techniques de sécurité (audits d'architecture, audits de vulnérabilités, tests d'intrusion, audits de code, etc.)
- Référentiels / Outils de management

