# SWIFT – Customer Security Programme

**Citizen Can** Corporate - Immeuble Charlebourg - Bât. C - 14/30 rue de Mantes - 92700 COLOMBES Tél : +33 (0) 1 47 84 75 86- Fax : +33 (0) 1 73 76 93 21 – E-mail : business@citizencan.fr
*RCS Nanterre 493 782 585 – Numéro de TVA Intracom FR 454 937 825 85*

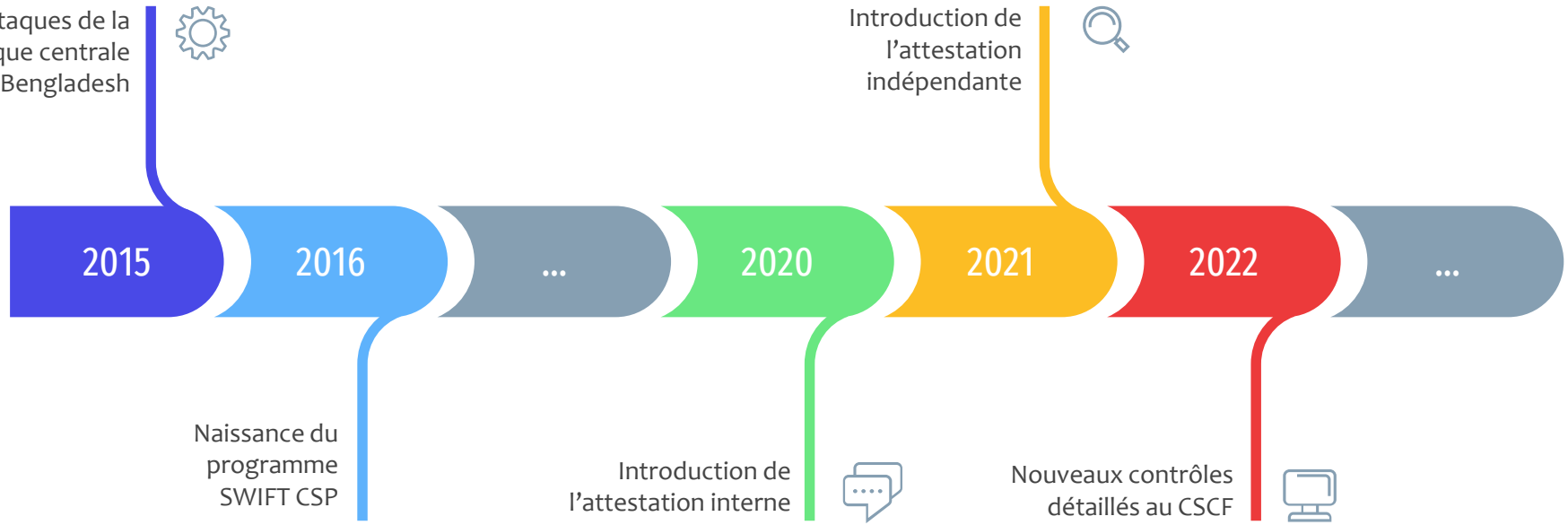
# SWIFT CSP - Chronologie

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 Programme).**

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 2023 a été publiée au début du mois de juillet 2022 et recense les mesures obligatoires et conseillées pour les attestations (déclaration à partir du mois de juillet 2023 lors de l'ouverture de la campagne dans l'application KYC-SA).

**Les clients SWIFT doivent se conformer chaque année au SWIFT CSCF publiée en juillet, en validant la déclaration au plus tard le 31 décembre.**



# SWIFT CSP - Périmètre


**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.

**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 2023 (Customer Security Controls Framework) et au-delà.

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

citizencan CORPORATE

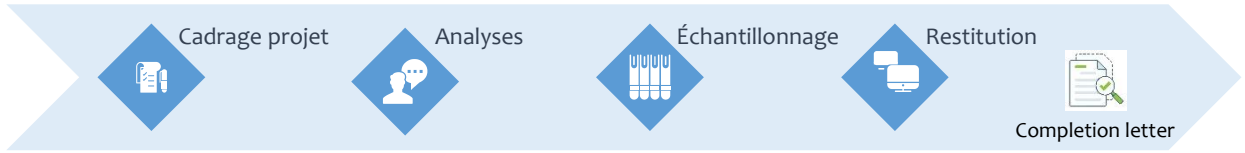
**La connaissance des Systèmes de Gestion de Trésorerie du marché**

**Spécialisé dans l'audit et l'évolution des Systèmes d'Information de Trésorerie**

CoESSI

**Spécialisé dans les audits techniques et de sécurité des Systèmes d'Information**

**Évaluateur indépendant externe Certifié ISO27001 et qualifié PASSI ***




## 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 2023

## *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
- Livrables identifiés : Customer Completion Letter, note de synthèse détaillant l'analyse fonctionnelle et technique réalisée

| | |
|---|---|
| 01 | Cadrage |
| 02 | Analyse documentaire |
| 03 | Ateliers complémentaires |
| 04 | Restitution |


### Certification proposée en forfait

- Audit fonctionnel et technique du programme CSP SWIFT 2023
- Production des livrables documentaires
- Pilotage de la mission, gouvernance simplifiée

# Liste des contrôles détaillés au CSCF

## *Mise à jour 2023 – 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

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

### Les points clés

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

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 citizencan entreprises citoyennes | citizencan entreprise citoyenne CORPORATE | citizencan entreprise citoyenne BANK | citizencan SPAIN

Entreprise B Certifiée

Citizen Can fait partie d'un mouvement mondial vers une économie plus inclusive, plus équitable et plus régénératrice.

PLATINUM Top 1% 2023 ecovadis Sustainability Rating

Citizen Can a obtenu le label PLATINIUM EcoVadis (Top 1%) sur sa performance RSE (Responsabilité Sociétale des Entreprises)

# Citizen Can Corporate

## *NOTRE OFFRE*

CITIZEN CAN CORPORATE, propose une assistance à maitrise d'ouvrage, ainsi qu'un accompagnement dans les projets de transformation de la fonction Trésorerie.

Les consultants du groupe sont spécialisés dans la conduite de projets Trésorerie et réalisent les actions suivantes :


- Audit et analyse des processus
- Conduite d'appel d'offres, aide à la décision
- Identification, gestion des risques et maîtrise de leurs conséquences


- Pilotage des projets, coordination des équipes
- Spécification et recette de la solution
- Conduite du changement, implémentation


- Documentation, transfert des compétences
- Gestion de la maintenance applicative
- Amélioration continue et pilotage des évolutions

## Quelques références

EIFFAGE
ALSTOM
SAUR
Schneider Electric
FINANCIERE AGACHE
europ assistance
DANONE
HERMÈS PARIS
B2Y GROUPE
L'ORÉAL GROUPE
FDJ
CHARGEURS
DATA LOG Think Cash
BUREAU VERITAS
SEVES
technicolor
malakoff humanis

# CoESSI

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