KPMG

SWIFT Customer Security Program

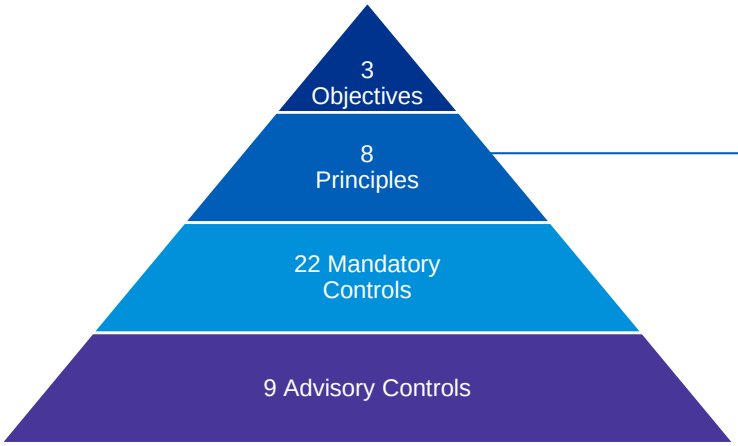
An introduction to SWIFT customer security controls framework (CSCF)

The financial sector continues to be a prime target for highly sophisticated, customized cyber-attacks. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) interbank messaging network has come under attack resulting in millions of dollars in losses for member financial institutions. In response, SWIFT has introduced a Customer Security Program (CSP) with a goal to strengthen the cyber security posture of the SWIFT payment network by increasing the cyber maturity of its members.

The SWIFT CSP is built around three pillars: (1) securing your local environment, (2) preventing and detecting fraud in your commercial relationships, and (3) continuously sharing information and preparing to defend against future cyber threats. As part of the CSP, SWIFT developed the Customer Security Controls Framework (CSCF) – a set of control guidelines for SWIFT members on how to securely operate their SWIFT environment. All its member organizations who use the interbank messaging network **must attest** with SWIFT's customer security controls framework (CSCF) on an annual basis.

What is the SWIFT Customer Security Program?

SWIFT adapts the framework to the changing threats as well as to the maturity of their membership. The SWIFT CSP requires each organization to define, document, implement and independently attest that their SWIFT environment is compliant with SWIFT's CSCF objectives, principles and controls. The v.2021 of the SWIFT CSCF comprises of 22 mandatory controls and 9 advisory controls to which members must self-attest their compliance.



SECURE YOUR ENVIRONMENT

- Restrict Internet Access
- Protect Critical Systems from the General IT Environment
- Reduce Attack Surfaces & Vulnerabilities
- Physically Secure the Environment

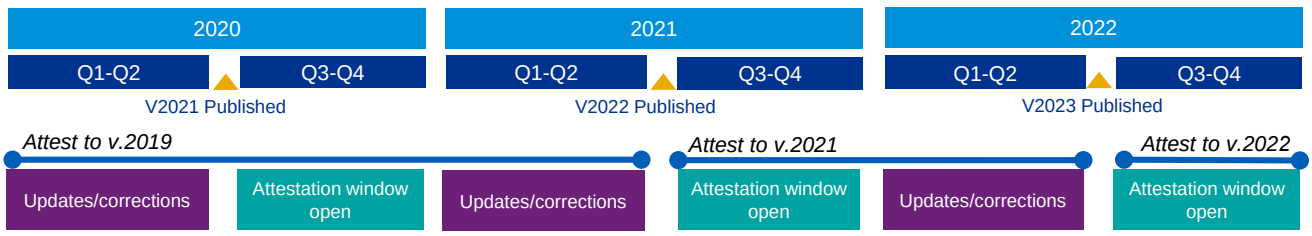
KNOW & LIMIT ACCESS

- Prevent Compromise of Credentials
- Manage Identities & Segregate Privileges

DETECT & RESPOND

- Detect Anomalous Activity to Systems or Transaction Records
- Plan for Incidence Response & Information Sharing

With the introduction of v.2021 of the CSCF, SWIFT has also published a timeline for members which provides a schedule for the introduction of changes to the framework and the reporting requirements. SWIFT member organizations will be expected to assess and implement these changes in accordance with the published timeline.



KPMG

How can we help?

An important change SWIFT introduced is that self-assessment is no longer an option for attestation. SWIFT members are required to have an independent assessment of the attestation status of their organization. The type of assessment can either be a review or an audit. These can be provided internally or externally, as long as sufficient evidence and independence can be demonstrated. Internal assessments can be conducted by risk management or internal audit functions – these can be supplemented with expert resources from companies such as KPMG. External assessments can provide clear independence in the assessment and provide additional confidence to both internal and external stakeholders.

SWIFT RISK ASSESSMENT AND READINESS REVIEW

KPMG will work with you to perform a gap assessment of your SWIFT environment, processes, controls and governance against the SWIFT CSCF assurance framework using KPMG's SWIFT Security Assessment (KSSA) framework. Our approach is to identify the most efficient way to maintain a unified posture between the SWIFT requirements and client controls to reduce duplication and overlap with existing transaction processing and cyber security controls.

REMEDIATION SERVICES

- Cyber Security transformation programs to remediate gaps
- Selection and implementation of SWIFT and Third-Party security tools
- independent vendor assessment and champion selection of cyber tools

ATTESTATION SERVICES

KPMG can assist an organization in preparing for and performing an attestation examination in accordance with the SWIFT CSCF criteria by performing one of the below:

- Attestation Examination (AT-C 205)
- International Attest (ISAE-3000)
- Dual Reporting Attestation (US & Int'l. Standard)
- SOC 2+ (including SWIFT CSCF Criteria)

Why KPMG?

56+ Number of countries with available KPMG resources (Cyber, Audit, SWIFT)

180+ Number of SWIFT CSP assessments and attestations performed in the US and globally since SWIFT CSP inception

180+ Number of SWIFT CSP practitioners and SWIFT SMEs in KPMG's global network

3200+ Cyber Security professionals available from our global Cyber team

KPMG is a recognized Global Consultancy Partner for SWIFT

Contact us

Ali Al-Shabibi
Partner
KPMG in Qatar
M: +974 7471 2768
E: aalshabibi@kpmg.com

Rami Hasan
Director
KPMG in Qatar
M: +974 5064 2787
E: ramihasan@Kpmg.Com

Suleiman Gammoh
Manager
KPMG in Qatar
M: +974 6625 3672
E: suleimangammoh@Kpmg.Com

Idrak Ahmad Khan
Assistant Manager
KPMG in Qatar
M: +974 3342 7638
E: idrakk@kpmg.com