KPMG

SWIFT Customer Security Controls Framework

Raising the Bar

May 2021

An introduction to SWIFT Customer Security Controls Framework (CSCF)

The financial sector continues to be a prime target for highly sophisticated, customized cyberattacks. The Society for Worldwide Interbank Financial (SWIFT) interbank messaging network has come under Telecommunications 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 cybersecurity posture of the SWIFT payment network by increasing the cyber maturity of its members. 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.

SWIFT CSCF Evolves

SWIFT adapts the framework to the changing threats as well as to the maturity of their membership.

The v.2021 of the SWIFT CSCF comprises 22 mandatory controls and 9 advisory controls to which members must self-attest their compliance. The CSCF has expanded both in terms of scope and with an additional control objective. The current iteration (v.2021) now includes the disaster recovery environment, and SWIFT has added another mandatory control objective for Restriction of Internet Access (1.4) and a new architecture type (A-4).

Additionally, SWIFT has published its Independent Assessment Framework, which mandates that all members must perform their assessment in an independent manner. Lastly, SWIFT has removed the 12-month expiry reporting cycle, now requiring only a year-end attest to SWIFT.

> “Cyberattacks are a major concern for the US financial firms because banks and other financial institutions experience up to 300 times more cyber incidents in a year than organizations in other sectors.”

Source: New York Federal Reserve Bank, Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis (Jan. 1, 2020);

The industry undergoing rapid transformational change and innovation, along with the increased scrutiny from regulators, and the evolving SWIFT framework pose significant risks to financial organizations to protect the authentication, integrity and confidentiality of transactions and their underlying technology platforms.

Additionally, other key elements to consider are as follows:

SWIFT reserves the right to report non-compliant members to their local regulators and counter-parties

SWIFT has begun selecting members to engage third parties to validate their attestation

Increased focus and scrutiny by regulators

How we can 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, which 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 additional confidence to both internal and external stakeholders.

SWIFT Readiness Review

KPMG can 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 cybersecurity controls.

SWIFT Independent Attestation

SWIFT mandates that all the members have to complete an independent attestation against their compliance on CSCF by 31 December 2021.

KPMG can assist an organization in preparing for and performing an attestation examination in accordance with the SWIFT CSCF criteria.

Tentative Roadmap for Financial Institutions

June 2021

SWIFT Readiness Assessment

▼

July – Aug 2021

Implementation of Gaps Identified during Readiness Assessment

▼

Oct 2021

SWIFT Attestation

▼

Dec 2021

Compliance with SWIFT Mandate

> *KPMG has been listed as an 'Assessment Provider' in Kuwait in the directory of Assessment Providers listed by SWIFT.*

Why KPMG

TRUSTED

We have worked with some of the largest companies in the world and delivered on complex global programs. You can trust in the quality of our approach and on receiving personal attention.

TRANSPARENT

We rely on transparent project execution, providing timely and adequate visibility to all the stakeholders, and ensure the best output through our multi-tiered quality assurance model.

RELEVANT

We have deep experience and right skills having worked with leading financial institutions around the world.

AWARD WINNING

Our Cyber Security team is award winning. KPMG has been named as a 'Leader' in the Forrester Research Inc. report for the Information Security Consulting Services, achieving the highest score for current offering and strategy.

LOCAL PRESENCE, GLOBAL REACH

KPMG is a global network of over 207,000 professionals in 154 countries. Through our worldwide network and local pool of cyber professionals, we have the ability to orchestrate and deliver consistently high standards for clients across the world.

Contacts

Ali Abbas
Director – Risk Consulting
M +965 5169 8765
T: +965 2228 7406
E: aliabbas@kpmg.com

Mithun Kalappura
Manager, IT Risk Consulting
T: +965 2228 7480
M: +965 9445 4264
E: mkalappura@kpmg.com

KPMG

Download on the App Store

kpmg.com/social media

kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.