KPMG

SWIFT Customer Security Programme Update

Stay trusted within the SWIFT network

What's new?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) released the Customer Security Controls Policy on May 19, which includes further information when it comes to the roles, responsibilities and process details of the customer security attestation and follow-up process. This document is an update to the Customer Security Programme (CSP) released. CSP aims to reinforce the security of the entire SWIFT ecosystem by improving the local environment security of each individual SWIFT user. To achieve this, SWIFT requires users to follow the two steps below:

1. **Self-assessment against the SWIFT Customer Security Controls Framework (CSCF)**: CSCF provides 16 mandatory security controls and 11 advisory security controls, which are recommended best practices. Users are required to self-assess their SWIFT local environments against CSCF annually. All 16 mandatory controls must be included, while users can choose to exclude the 11 advisory security controls from the self-assessment. KPMG, a global consultancy partner with SWIFT, can perform this self-assessment on a user's behalf.

2. **Self-attestation following the SWIFT Customer Security Controls Policy**: Users are required to submit a self-attestation on their compliance with the individual CSCF controls based on the self-assessment results (The 11 advisory security controls can be excluded from the self-attestation). The self-attestation is submitted through SWIFT's online portal - KYC Registry Security Attestation Application. The first self-attestation must be submitted by 31 December 2017, and annually thereafter.

What if a user does not comply?

Failure to submit self-attestation is visible to all counterparties

Details of a user's compliance with individual CSCF controls are by default restricted from its counterparties in the KYC Registry Security Attestation Application unless specific access is granted by the user. However, the presence or absence of a submitted self-attestation is visible to the counterparties. It is therefore essential to perform both self-assessment and self-attestation.

SWIFT can report a user's non-compliance to local supervisory bodies*

Starting from 2018, SWIFT can report a user's late submission or absence from the first self-attestation to local supervisory bodies - for banks in Hong Kong, the local supervisory body is the Hong Kong Monetary Authority (HKMA), whereas the Securities and Futures Commission (SFC) oversees securities firms in the city.

SWIFT will also begin reporting a user's failure to fully comply with the CSCF mandatory security controls to local supervisory bodies in 2019. It is imperative for any issues identified in a self-assessment to be addressed quickly.

SWIFT can report a user's non-compliance to messaging counterparties*

For those without a direct local supervisory body, SWIFT can report the user's non-compliance status to their messaging counterparties instead.

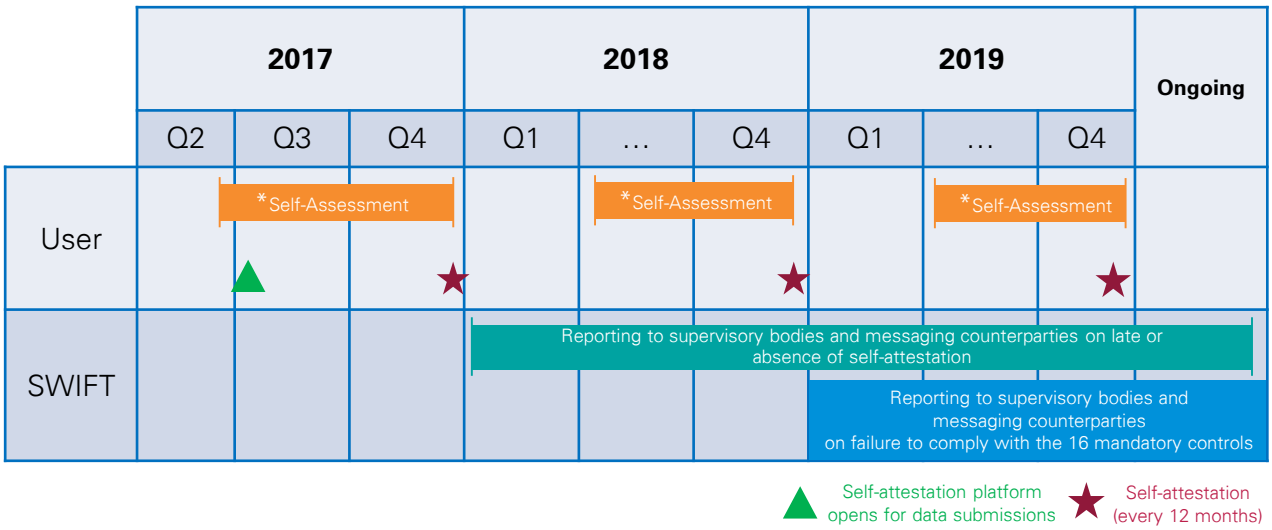
**Note: if the user engages a non-compliant SWIFT service provider, SWIFT can also report this to supervisory bodies and other messaging counterparties.*

What should a user do to comply?

SWIFT users should perform an annual self-assessment of their security environment against the CSCF requirements. They would then need to follow up by providing their self-attestation* of their compliance status against the CSCP mandatory controls via the KYC Registry Security Attestation Application.

*Note: if there are material changes to the user's SWIFT implementation (e.g. change of architecture type or service provider), the user is required to perform a self-assessment and submit a new self-attestation within a month of the change.

CSP Timeline



CSCF overview

The annual self-assessments and self-attestations are performed against SWIFT's CSCF requirements:

3 Objectives	8 Principles	27 controls
Secure your environment	1. Restrict internet access 2. Protect critical systems from the general IT environment 3. Reduce attack surfaces and vulnerabilities 4. Physically secure the environment	• There are 16 mandatory controls, and 11 optional controls • SWIFT recommends the implementation of CSCF controls on the entire end-to-end transaction chain beyond the SWIFT local infrastructure, e.g. the upstream payment processing systems • Controls are mapped against recognised international standards where applicable – NIST, PCI-DSS and ISO 27002. Complying with these standards would indicate that a SWIFT local infrastructure is, to some extent, compliant with CSCF
Know and limit access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges	
Detect and respond	7. Detect anomalous system activity or transaction records 8. Plan for incident response and information sharing	

Source: adapted from SWIFT

What does this means to a user now?

Users need to be aware of the time it takes to perform a self-assessment and self-attestation. As a result, they need to immediately review the CSCF, identify control gaps in their local SWIFT environments, and establish plans to implement or reinforce the controls.

How can KPMG help

1. SWIFT Readiness Review

In preparation for your self-assessment, KPMG's security specialists will perform a gap assessment of your SWIFT controls against the CSCF requirements. We can also perform vulnerability scanning and penetration testing for all related SWIFT applications and interfaces. Users will have ample time to remediate gaps identified in this review in preparation for the self-assessment.

2. SWIFT Remediation Services

KPMG can perform cyber security transformation programmes to remediate identified gaps. We can also select and implement SWIFT and other third party security tools, or perform independent vendor assessment and selection for tool deployments.

3. SWIFT Assessment Services

KPMG can act as an external service provider to perform the initial, and subsequent annual self-assessments on your behalf.

Stronger security posture

Your organisation's security posture will improve by implementing the recommendations from KPMG's remediation and assessment services.

Self-attestation compliant

An improved security posture will naturally lead to a higher level of compliance for the annual self-attestation.

Why KPMG?

Cyber security is a key strategic focus of KPMG. Our dedicated team of cyber security specialists and our SWIFT assessment framework provides a globally validated and consistent approach to help companies achieve optimal value.

A global SWIFT partner

KPMG is a global SWIFT partner. We possess:

- Extensive cyber security services experience and credentials
- A strategic focus on cyber security services
- A strong reputation and commitment towards the financial industry.

KPMG's security specialists have access to the latest SWIFT standards and requirements and will be notified of any changes at the earliest opportunity.

Dedicated SWIFT assessment framework

KPMG has a SWIFT-specific global framework based on:

- KPMG's assurance and cyber security frameworks
- SWIFT Customer Security Control Framework
- SWIFT audit guidelines
- Leading international practices

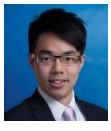
The assessment framework covers SWIFT-specific controls and SWIFT underlying infrastructure.

Contact us

Henry Shek
Partner
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Richard Zhang
Director
KPMG China
T: +86 (21) 2212 3637
E: richard.zhang@kpmg.com

Jason He
Director
KPMG China
T: +86 (755) 2547 1129
E: jason.rk.he@kpmg.com



Alvin Li
Associate Director
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Frank Xiao
Associate Director
KPMG China
T: +86 (10) 8508 5456
E: frank.xiao@kpmg.com

kpmg.com/cn