SWIFT - Customer Security Programme (CSP)

The financial sector continues to be a prime target for highly sophisticated, customised attacks. In February 2016, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) money transfer system came under attack, resulting in a multi-million heist at one of the central banks. Additional attacks have been reported at a number of different financial institutions.

In response, SWIFT has introduced a Customer Security Program (CSP) that requires all organisations who use the interbank messaging network to comply with core security standards – as well as a related "assurance framework". SWIFT is introducing this program to improve information sharing between members, enhance SWIFT-related tools and provide the community with a standardised assurance framework.

What is the SWIFT Customer Security Programme?

The SWIFT CSP requires every member organisation to define, document, implement and attest that their SWIFT messaging environment is compliant with SWIFT's CSP objectives, principles and controls as provided in the table below. The 16 mandatory and 11 advisory controls will underpin the 8 principles.

SWIFT Customer Security Programme

3 objectives	8 principles	27 controls
Secure your environment	1. Restrict internet access 2. Protect critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment	— Applicable to all customers and to the whole local SWIFT infrastructure — Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002 — Some controls are mandatory, some are advisory — Documentation and collateral will be available by April 2017
Know and limit access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges	
Detect and respond	7. Detect anomalous activity to system or transaction records 8. Plan for incident response and information sharing	

Source: SWIFT

In March 2017 SWIFT released cyber security standards with inspections and enforcement beginning in January 2018. All organisations that use SWIFT, not just financial institutions, must attest that they comply with the standards, on an annual basis, or face being reported, not just to their regulators, but also other SWIFT members. In the later phases of the programme, in addition to self-attestation, SWIFT will require additional assurance from their members, using internal and external auditors to perform testing over the SWIFT CSP controls.

How can KPMG help?

SWIFT readiness assessment

Our team will work with key payment and wire transfer business, IT, legal, compliance, security, privacy and risk management stakeholders to determine the scope and perform a gap assessment of the SWIFT environment, processes, controls and governance against the SWIFT CSP objectives, principles and controls. We will advise on the most efficient and effective way to design and implement additional controls to close any gaps with the SWIFT CSP and map them to international standards such as NIST, PCI-DSS, and ISO 27002.

SWIFT controls implementation

Our team of professionals will provide post-assessment advice and implementation support covering all areas of the SWIFT CSP controls; integrating the new controls into your organisation's existing SWIFT payment and wire transfer processes. This will include the design and development of processes, policies, procedures and technology architectures for the 3 SWIFT Customer Security Program objectives:

— Secure your environment;
— Know and limit access; and
— Detect and response

SWIFT attestation services

The SWIFT CSP has adopted an assurance framework that will be deployed; requiring a detailed proof of compliance from the member organisations. We will assist an organisation in preparing for and performing the SWIFT CSP attestation, which can be in the form of:

— Self-attestation assistance
— Self-inspection assistance
— Service organisation controls reporting under standards such as ISAE 3000 or SOC 2

Other SWIFT services

Cyber security awareness training and phishing exercise

People are the most valuable asset for every organisation, but at the same time they provide a major attack vector for individuals and organisations with malicious intentions. That is why security training and awareness is a mandatory control within the SWIFT CSP. KPMG will help you and your organisation achieve compliance with this SWIFT CSP requirement by delivering tailored cyber security training and by conducting phishing campaigns.

Penetration testing of the SWIFT infrastructure

Penetration testing is one of the advisory controls within the SWIFT Customer Security Program and is also one of the standard KPMG services. We design and tailor each penetration test so that it will help you identify critical areas and key vulnerabilities, guiding your mitigation efforts. We will focus on systems and services within the SWIFT CSP scope and any part of your IT environment, as may be required.

Cyber maturity assessment (CMA)

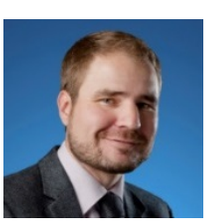
CMA provides an in-depth review of an organisation's ability to protect its information assets and its preparedness against cyber threats. It is unique in the market in that it looks beyond pure technical preparedness for cyber threats. It takes a rounded view of people, process and technology to enable clients to understand areas of vulnerability, to identify and prioritise areas for remediation and to demonstrate both corporate and operational compliance, turning information risk to business advantage

How KPMG can help?

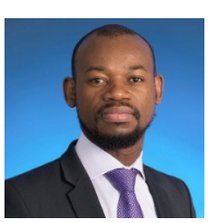
We will assist SWIFT member organisations in complying with the SWIFT security requirements by providing them with a tailored approach. We will employ a cross-functional team of subject matter professionals in IT audit, assurance and cyber security, who are familiar with and have experience in the financial services industry.

Contact us

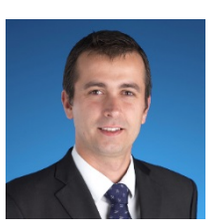
Brian Bethell
Director, Audit
+44 (0)1534 608405
brianbethell@kpmg.com



Teijo Peltoniemi
Senior Manager, Digital
+44 (0)1534 632565
teijopeltoniemi@kpmg.com



Arthur Mainja
Senior Manager, Digital
+44 (0)1534 632551
amainja@kpmg.com



Matej Jurkic
Manager, Digital
+44 (0)1481 755787
mjurkic@kpmg.com

www.kpmg.com/channelislands