SWIFT Customer Security Programme

The essentials

November 2020

What is the SWIFT Customer Security Programme?

SWIFT Customer Security Programme (CSP)

SWIFT has introduced its Customer Security Controls Framework (CSCF) to drive security improvement and transparency across the global financial community. The SWIFT CSP focuses on three mutually reinforcing areas. Protecting and securing your local environment, preventing and detecting fraud in your commercial relationships, and continuously sharing information and preparing to defend against future cyber threats.

While all customers remain primarily responsible for protecting their own environments, SWIFT's CSP aims to support its community in the fight against cyber-attacks.

Why is it important?

In response to a number of cyber attacks and breaches throughout 2016, SWIFT identified, in 2017, 16 mandatory and 11 optional security controls for all its 11,000 customers worldwide. All customers are asked to attest to meeting the controls on an annual basis, with results shared with counterparts and regulators.

How will this impact SWIFT customers?

The SWIFT CSP has evolved, and will continue to do so, since the inception of the CSP. Customers will need to continue to implement security controls and raise the bar to ensure compliance with the CSCF. Previously, SWIFT customers were required to self-attest to the CSCF V2019 by 31 December 2019. This updated framework contained 19 mandatory and 10 advisory security controls.

In 2020*, SWIFT promoted two existing advisory controls to mandatory and introduced two new advisory controls resulting in 21 mandatory and 10 advisory controls in the CSCF V2020. For 2021, SWIFT promoted one control to mandatory resulting in 22 mandatory and nine advisory controls in the CSCF v2021. All SWIFT users will be required to perform an 'independent assessment' as it is a key requirement of their annual self-attestation to demonstrate their compliance with the SWIFT CSP.

What are the success factors?

To be successful, organisations must take a thoughtful and systematic approach, requiring collaboration across the three lines of defence, strong leadership and a diverse organised team.

How is the SWIFT CSP framework structured?

Security principles	Controls objectives	Controls

Description – Includes items such as control frequency, who or what performs the action, what action was performed and what action or effect is the result.

Components – Includes specific people, process and technology elements associate with the control.

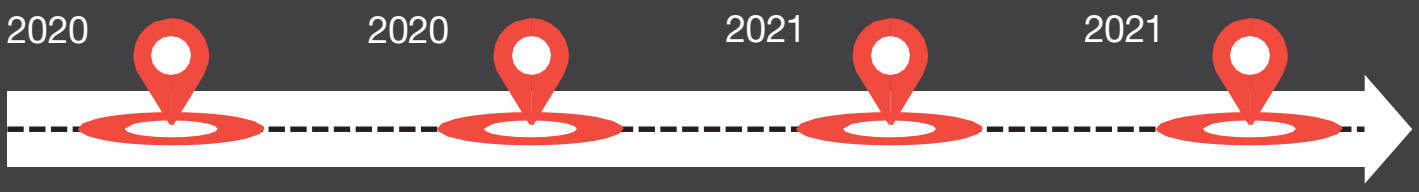
Validation measures – Includes the method by which control design and effectiveness will be validated, the frequency and associated artefacts.

Owner – Includes information related to the control owner such as name and functional title.

pwc

* Given the global COVID-19 situation, SWIFT has published updated guidelines on 18 June 2020 regarding changes to the CSP self-attestation and independent assessment requirements for 2020. SWIFT has announced that in 2020, customers can self-attest against the 2019 version of the SWIFT CSP and can optionally support the self-attestation with an independent assessment. In 2021, independent assessment will be a mandatory requirement and customers will be required to attest against the 2021 version of the CSP framework.

What milestones should you be aware of?



Annual attestation

Comply with the CSCF v2019 or optionally against the CSCF v2020 framework

Self-attestation submission

SWIFT will require all organisations to submit their attestation for 2020 by 31 Dec 2020

SWIFT CSP v 2021

Customers must comply with CSCF v2021 including 22 mandatory and 9 advisory controls

Independent assessment

SWIFT requires all customers to support their attestation with an independent assessment by the end of 2021

PwC capabilities

How can PwC help to meet SWIFT's independent assessment?

SWIFT CSP audit

Validation of successful alignment of controls with the SWIFT CSP guidelines resulting in a controls report under recognised standards (e.g. ISAE3000)

SWIFT CSP assessment

A detailed assessment of SWIFT CSP controls by leveraging our CSP accelerator

Embedded in internal audit

Work alongside your internal audit function to report on SWIFT CSP controls

Additional cyber security services

Penetration testing	**Red-team testing**	**Technical benchmarking**	**Breach indicator assessments**

Why PwC?

Proven CSP assurance experience

We've performed numerous SWIFT CSP assurance engagements across multiple territories and industries.

Cohesive team who understands SWIFT

We understand SWIFT like no other as we performed an annual review of SWIFT under the internationally recognised ISAE3000 standard for over 10 years.

Technical expertise and knowledge base

We're the only 'Big-4' firm with a professional Certified Cyber Security Consultancy certificate from the NCSC. We're unique in our ability to leverage threat intelligence to build and simulate realistic cyber-attack scenarios.

Adapting to your requirements

PwC will leverage inhouse accelerators and our extensive SWIFT CSP expertise to ensure that your needs are met ahead of SWIFTs required independent assessment due on 31 December 2021.

Contacts

Chris Eaton
Advisory Director
M: +44 7797 900015
E: chris.eaton@pwc.com

Kevin Thompson
Advisory Senior Manager
M: +44 7797 915430
E: kevin.thompson@pwc.com

For further information refer to:
www.pwc.com/jg/