SWIFT Customer Security Programme
The essentials

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?

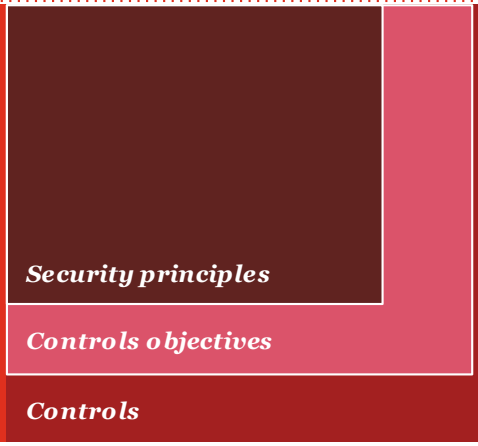
The SWIFT CSCF has evolved, and will continue to do so, since the inception of the CSP. Customers will need to continue to implement security controls and raise the bar to ensure compliance with the CSCF. Previously, SWIFT customers were required to self-attest to the CSCF V2019 by 31 December 2019.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

For 2020, SWIFT promoted 2 existing advisory controls to mandatory and introduced 2 additional advisory controls resulting in 21 mandatory and 10 advisory controls in the CSCF V2020. 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 CSCF. The self-attestation for 2020 is due on 31 December 2020.

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?



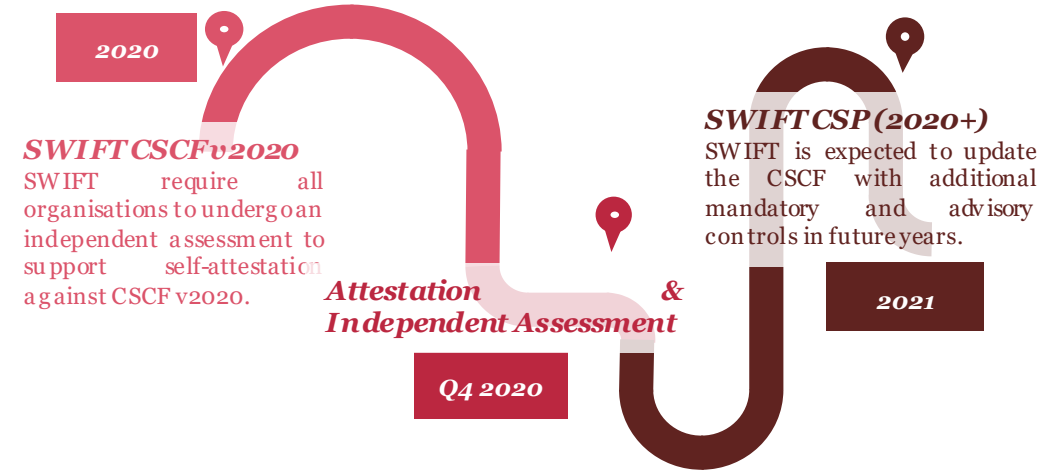
Description – *Includes items such as control frequency, who or what performs the action, what action was performed and what action or effect is the result.*

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.*

What milestones should you be aware of?



SWIFT Customer Security Programme
PwC capabilities

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

Swift CSP Audit — 1

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 — 2

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

Embedded in Internal Audit — 3

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

Additional Cyber Security services

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

Why PwC?

Cohesive team who understand SWIFT	*PwC understands SWIFT like no other as we have been performing an annual review of SWIFT under the internationally recognised ISAE3000 standard for over 10 years.*
Proven performance on similar projects	*PwC have performed numerous SWIFT CSP security assessments worldwide and as such, we have a proven approach and understanding of how to ensure the security of SWIFT infrastructure, while maintaining functionality.*
Technical expertise and knowledge base	*PwC is the only 'Big-4' firm with a professional Certified Cyber Security Consultancy certificate from the NCSC. PwC are unique in our ability to leverage threat intelligence to build and simulate realistic cyber attack scenarios.*
Adapting to your requirements	*PwC will formulate and tailor an approach that adapts to your requirements and SWIFT's needs for the 2020 Independent Assessment. PwC will provide pragmatic insights and balanced views on how to prioritise any associated actions.*

David Woerndl
Global SWIFT CSP Lead
M: +44 (0)7809 756281
E: david.woerndl@pwc.com

Alessandro Frenza
Global SWIFT CSP Lead (Cyber Security)
M: +44 (0)7493 319240
E: alessandro.frenza@pwc.com

Hattie Johnstone-Browne
Global SWIFT CSP SME
M: +44 (0)7802 659300
E: hattie.johnstone-browne@pwc.com

Rishabh Rastogi
Global SWIFT CSP SME
M: +44 (0)7725 068141
E: rishabh.rastogi@pwc.com

For further information refer to: www.pwc.co.uk/swift