SWIFT security attestation: Meet this year's deadline

protiviti®
Global Business Consulting

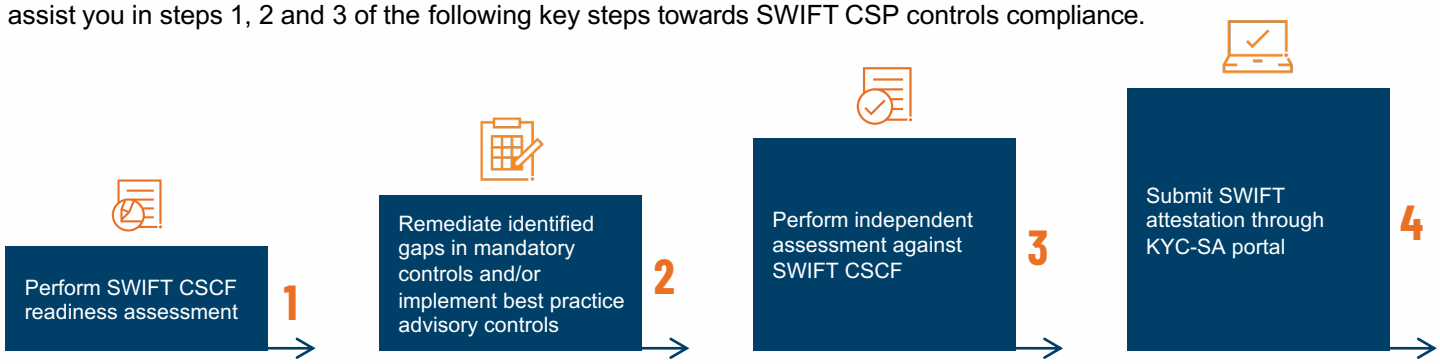
Is your organisation equipped to meet the 31 December 2024 compliance deadline?

Background

- SWIFT has revised counterparty requirements to include an independent assessment as part of the **annual counterparty attestation process**
- A SWIFT attestation is an assessment that ensures organisations meet satisfactory compliance levels against the SWIFT Customer Security Controls Framework (CSCF) as part of the mandated Customer Security Program (CSP), founded on industry accepted principles (**PCI-DSS, ISO27001** and **NIST**)
- All counterparties must attest before the expiry date of the current control's version, confirming full compliance with the mandatory security controls no later than **31 December each year**
- The independent assessment can be performed internally by qualified (e.g., QSA, CISSP, CISA, etc.) internal individuals and/or external SWIFT CSP Certified Assessor(s).

STEPS TO COMPLIANCE

Protiviti's Certified Assessors and SWIFT professionals can help your organisation address the SWIFT independent assessment with our experience in working with various SWIFT counterparties locally and internationally. Protiviti can assist you in steps 1, 2 and 3 of the following key steps towards SWIFT CSP controls compliance.



HOW CAN PROTIVITI HELP?

Secure your environment

Perform an independent or joint assessment in step 3 of the lifecycle. To analyse current control environments to determine if controls satisfy SWIFT CSP requirements and allow customers to submit their Know Your Customer – Self Attestation (KYC-SA).

Strategy and implementation

Assist SWIFT counterparties with remediation of identified gaps in mandatory controls (refer to appendix for a structured breakdown of mandatory controls) or implementing best practice advisory CSP controls within their SWIFT environment and strategic transitions.

Independent or co-source assessment

Perform the independent assessment leveraging an outsourced or co-sourced delivery model.

Appendix

KEY CONSIDERATIONS IN ADHERING TO THE SWIFT CSP

Architecture and mandatory control types

A1

Users owning the communication interface (and generally the messaging interface)

A2

Users owning the messaging interface but not the communications interface

A3

SWIFT Connector is used within the user environment to facilitate application-to application communication with an interface at a service provider or with SWIFT services

A4

Customer Connector, a server running software application is used within the user environment to facilitate application-to-application communication with an interface at a service provide.

B

No local user footprint, no SWIFT-specific infrastructure component is used within the user environment.

24 controls	24 controls	23 controls	20 controls	17 controls

Mandatory and advisory security controls	Architecture type				
	A1	A2	A3	A4	B
1 Restrict internet access and protect critical system from general IT environment					
1.1 Swift environment protection					
1.2 Operating system privileged account control					
1.3 Virtualisation or cloud platform protection					
1.4 Restriction of internet access					
1.5 Customer environment protection					
2 Reduce attacks and surface vulnerabilities					
2.1 Internal data flow security					
2.2 Security updates					
2.3 System hardening					
2.4A Back office data flow security					
2.5A External transmission data protection					
2.6 Operator session confidentiality and integrity					
2.7 Vulnerability scanning					
2.8 Outsourced critical activity protection					
2.9 Transaction business controls					
2.10 Application hardening					
2.11A RMA business controls					
3 Physically secure the environment					
3.1 Physical security					

Mandatory and advisory security controls	Architecture type				
	A1	A2	A3	A4	B
4 Prevent compromise of credentials					
4.1 Password policy					
4.2 Multi-factor authentication					
5 Manage identities and separate privileges					
5.1 Logical access control					
5.2 Token management					
5.3A Staff screening process					
5.4 Password repository protection					
6 Detect anomalous activity to systems or transaction records					
6.1 Malware protection					
6.2 Software integrity					
6.3 Database integrity					
6.4 Logging and monitoring					
6.5A Intrusion detection					
7 Plan for incident response and information sharing					
7.1 Cyber incident response planning					
7.2 Security training and awareness					
7.3A Penetration testing					
7.4A Scenario-based risk assessment					

CONTACT US

Ghislaine Entwisle

Managing Director
Protiviti Australia
+61 431 285 494
Ghislaine.Entwisle@protiviti.com.au

Jeff Ho (Lead Assessor)

Associate Director
Protiviti Australia
+61 468 867 166
Jeff.Ho@protiviti.com.au

Hendrik Viljoen

Senior Manager
Protiviti Australia
+61 493 363 496
Hendrik.Viljoen@protiviti.com.au

protiviti®