Deloitte.

Deloitte SWIFT Customer Security Program experience

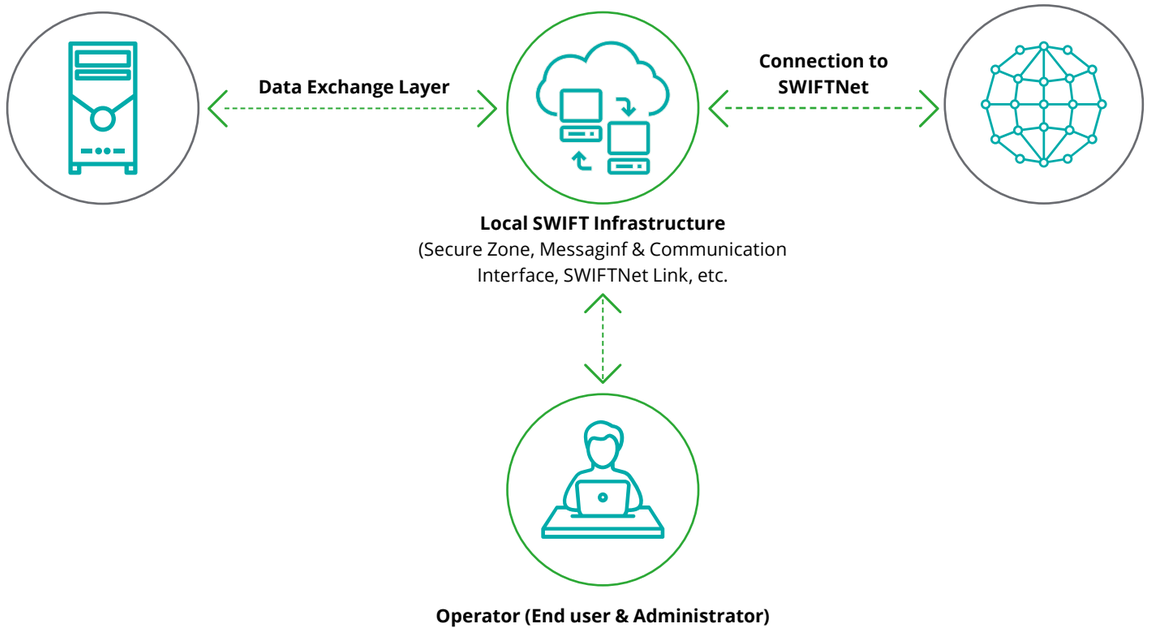
SWIFT Customer Security Controls Framework and applicability

The Customer Security Controls Framework is a set of core security controls that are mandatory for SWIFT users. The controls are intended to help mitigate specific cybersecurity risks that SWIFT users face due to the cyber threat landscape. Examples include unauthorized sending or modification of financial transactions, processing of altered or unauthorized SWIFT messages, etc.

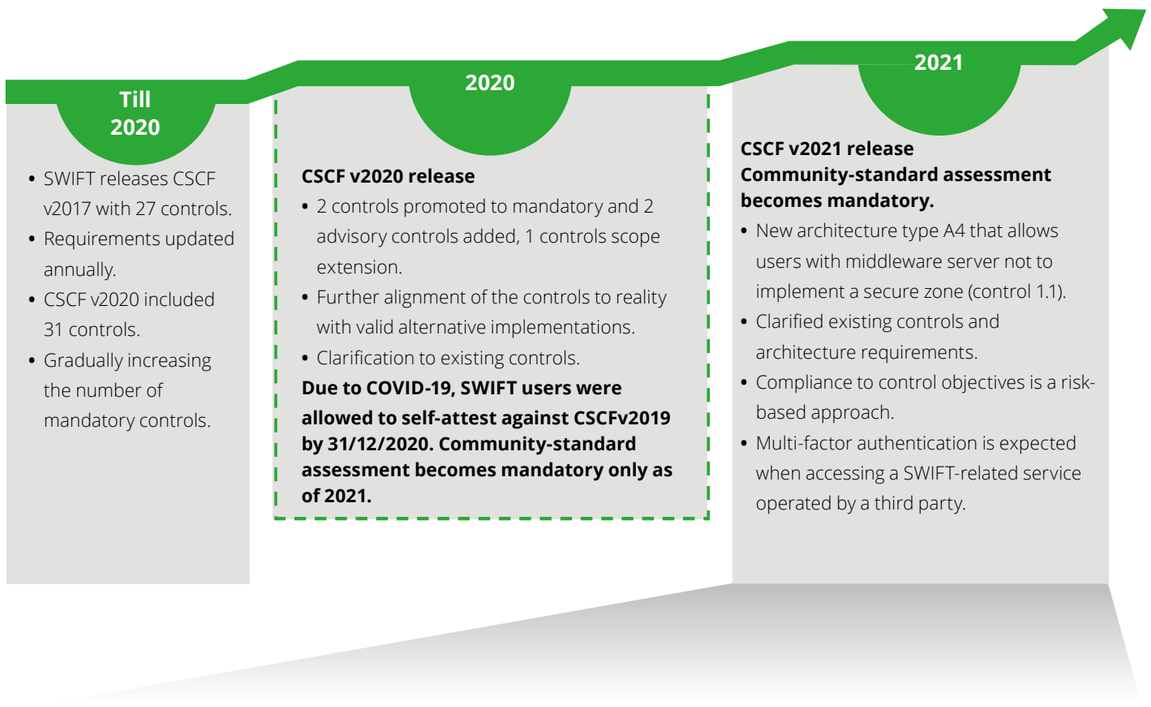
SWIFT Customer Security Controls Framework

Objectives	Strategic Security Principles
O1. Secure Your Environment	P1. Restrict Internet access and Protect critical systems from general IT environment
	P2. Reduce attack surface & vulnerabilities
	P3. Physically secure the environment
O2. Know and Limit Access	P4. Prevent compromise of credentials
	P5. Manage identities & segregate privileges
O3. Detect and Respond	P6. Detect anomalous activity to system or transaction records
	P7. Plan for incident response & information sharing

Scope of SWIFT Security Controls



Critical activities to meet CSP milestones



Our experience and credentials

Unique Customer Security Controls Framework CSCF credentials (framework used for SWIFT CSP)
Deloitte has a unique set of credentials built in our role as the sole entity that performs assessments of operational and security requirements of SWIFT Service Bureau and Lite 2 Business Application Providers (financial messaging connectivity providers). These providers are assessed against a framework that is based on SWIFT CSCF.

As part of this program Deloitte performed so far assessments based on SWIFT CSCF around the globe of more than 100 financial messaging services connectivity providers and Lite 2 Business Application Providers.

Deloitte SWIFT CSP Centre of Excellence
In order to deliver the highest quality of service across regions and build upon our experience Deloitte has established a SWIFT CSP center of excellence with a professionals skilled and experienced in security projects based on SWIFT Customer Security Controls Framework (CSCF). Our experts executed the projects from start to end, or supported local Deloitte offices as subject matter experts in delivering the security assessments based on CSCF.

SWIFT CSP tailor made methodology
Deloitte has a strong track record of performing operational and security risk assessments based on the SWIFT CSCF. Using that experience we created a tailor made methodology based on SWIFT CSCF and international security standards specific for this type of engagements.

Selection of relevant experience

Client	Relevant experience
Provider of secure financial messaging services	Security assessment review program based on SWIFT Customer Security Controls Framework for a global financial messaging provider. As part of this program we have assessed more than 100 financial messaging services connectivity providers across the world.
Provider of secure financial messaging services	Lite 2 Business Application Providers Inspections – Delivery of more than 10 assessments of Lite 2 Business Application (financial messaging connectivity providers) in terms of operational compliance, on behalf of the financial messaging connectivity provider.
Provider of secure financial messaging services	Deloitte provided Quality Assurance to the provider of secure financial messaging services with their Customer Security Program (CSP). The goal of CSP is to reinforce the security of clients' wider ecosystem by engaging with its customers to make sure the security of their locally managed infrastructure is up to par. Deloitte helped to analyze the attestation data and report on the findings. Further, Deloitte advised on improvement of the program.
Central banks in Europe and Asia	Review for self-assessment of the internal controls relevant to the SWIFT environment in place at the bank and their (controls) compliance with the mandatory controls as published by SWIFT in the Customer Security Programme framework.
Major Nonprofit Organization	Cyber security review, taking into account SWIFT CSP, of SWIFT environment after infrastructure change.
Several major banks across EMEA region	Review of self-assessment related to the internal controls relevant to the SWIFT environment in place at the bank, and their compliance with SWIFT Customer Security Programme framework.
Major International Financial Institution	Review of the cyber security controls for the SWIFT payments applications environment, including a review of controls at a third party.

Contact us

Deloitte Luxembourg

Stéphane Hurtaud
Partner
Information &
Technology Risk
+352 45145 4434
shurtaud@deloitte.lu

Maxime Vérac
Director
Information &
Technology Risk
+352 45145 4258
mverac@deloitte.lu

Deloitte Global

Bert Truyman
Partner
SWIFT Directory of
the Assessors
+32 497 51 55 12
btruyman@deloitte.com

Deloitte.

46350