Deloitte.

SWIFT Customer Security Programme

Deloitte Risk Management

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	Staregic Security Principles
01. 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
02. Know and Limit Access	P4. Prevent compromise of credentials
	P5. Manage identities & segregate privileges
03. Detect and Respond	P6. Detect anomalous activity to system or transaction records
	P7. Plan for incident response

2021

What 2021 will bring

The self-attestation based on community Standard Assessment is **mandatory** as of 2021.

What is the community standard assessment?

The community standard assessment is an assessment by an **independent third party** (such as Deloitte) or your internal second- or third-line of defense such as your internal compliance, internal risk or internal audit departments (independent from the first-line of defense submitting the self-attestation).

Critical activities to meet CSP milestones in 2021 and onwards

2020

CSCF v2020 release

- 2 controls promoted to mandatory and 2 advisory controls added, 1 controls scope extension.
- Further alignment of the controls to reality with valid alternative implementations.
- Clarification to existing controls.

Due to COVID-19, SWIFT users were allowed to self-attest against CSCFvFv2019 by 31/12/2020. Community-standard assessment becomes mandatory only as of 2021.

2021

CSCF v2021 release
Community-standard assessment becomes mandatory

- New architecture type A4 that allows users with middleware server not to implement a secure zone (control 1.1).
- Clarified existing controls and architecture requirements.
- Compliance to control objectives is a risk-based approach.
- Multi- factor authentication is expected when accessing a SWIFT-related service operated by a third party.

31 Control in 2021

New architecture type A4 introduced

Self-Attestation by 12/31/2021

1 control promoted to mandatory

MFA on SWIFT related services operated by a third party

Connector definition updated

Unique Customer Security Controls Framework CSCF credentials (framework used for SWIFT CSP)

As part of this program so far, Deloitte performed, more than 100 assessments based on SWIFT CSCF around the globe.

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.

> *At Deloitte, we are uniquely positioned with credentials through which we can bring your organization with unprecedented insights into your SWIFT infrastructure. Do not hesitate to contact our subject matter experts for further information.*

Contact

Jakub Höll
Manager
+420 734 353 815
jholl@deloittece.com

Jakub Ponec
Senior Consultant
+420 773 768 762
jponec@deloittece.com