Deloitte.

The 2021 SWIFT CSP Update and its Impact

SWIFT CSP Changes in 2021

What is the impact of the updates of the 2021 version of the CSCF on your financial organisation

The SWIFT Customer Security Programme was created to set the bar of cyber security for the financial services industry, following a series of cyber heists. In this article, we look at the most recent changes that were made to the Customer Security Control Framework (CSCF) in order to maintain an up to date cyber security maturity in the financial industry. You may have some questions around this. How do the 2021 changes to the CSCF affect your organisation? What are the updates to the CSCF in 2021? When will we have to attest against the 2021 CSCF?

In this article we will have a more detailed look at what these changes are and how it affects your organisation.

History of the Customer Security Controls Framework

The customer security Controls Framework (CSCF) has gradually evolved over the past years. In a few years' time, the framework has emerged from including 27 controls in 2017, to 31 controls in 2021. Moreover, every year the number of mandatory controls increased. Typically there is a period of 18 months to understand and implement future changes to the framework. More specifically, the new version of the CSCF was released in June 2020 and compliance is expected by December 2021. In addition, the CSCF change management process allows a phased approach: new mandatory controls or scope extensions are typically first introduced as advisory and only thereafter as mandatory.

Over time, more controls will transform to mandatory controls and will have to be implemented. Therefore, we advise you to already start testing your readiness of those controls. By doing this, there is the added value of improving the maturity of the controls before they actually become mandatory. This avoids non-compliance with the Customer Security Programme in the future.

This year, the usual timelines were changed by SWIFT, in light of the current Covid-19 pandemic. Concretely, this means for you as an organisation that the self-attestation between July and December 2020, can be re-attested against the CSCFv2019, instead of the CSCFv2020. This will give you time to focus on business continuity.

Changed to be taken into account for your organisation:

1. Significant scope change

The scope of control 4.2 was significantly changed as multi-factor authentication is also to be presented when accessing, at least for transaction processing, a SWIFT related service, application or component operated by a service provider (such as a service bureau, an L2BA provider or intermediate actor). This means that authentication to any application used for SWIFT transaction processing, now requires multi-factor authentication.

2. New architecture types

One of the most significant changes of the updated version of the CSCF is the new architecture type: Type A4. The most important change here is that organisations that define themselves as an A4 type architecture, don't create a separate secure zone.

3. Advisory controls that are promoted to mandatory

Control 1.4 about the restriction of internet access has been promoted to a mandatory control for all infrastructure types. Direct access to the Internet raises exposure to internet-based attacks. Risk is even higher in case of human interactions (browsing, emails or other social network activities being permitted). Therefore, general purpose and dedicated operator PCs as well as systems within the secure zone have controlled direct internet access in line with business requirements.

The 2021 SWIFT CSP Update and its Impact | June 2021

SWIFT CSP Changes in 2021

4. Scope update and clarifications

The scope of 6 controls were extended with, for most cases, the (customer) connector. SWIFT has also clarified the definition of the 'connector': "Embed middleware/MQ servers and API end points when used to connect or transmit transactions to service providers or SWIFT

Differentiate SWIFT related connectors (such as SIL, DirectLink, AutoCLient).

Additionally, an explicit reference was added to remote (externally hosted or operated) virtualisation platform to foster attention when engaging with a third party or moving to the cloud under requirement 1.3.

With COVID-19, SWIFT users are allowed to self-attest against the 2019 version of the CSCF by the end of 2020. The self-attestation based on community Standard Assessment is mandatory only 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 defence such as your internal compliance, internal risk or internal audit departments (independent from the first-line of defence submitting the self-attestation).

At Deloitte Africa, we are uniquely positioned with credentials through which we can bring your organisation with unprecedented insights into your SWIFT infrastructure. Do not hesitate to contact our subject matter experts for further information via our **website** or personally by reaching out to **Tiaan van Schalkwyk or Deena Chetty**

CONTACTS

Southern Africa

Navin Sing
Managing Director | Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Shahil Kanjee
Risk Advisory Africa | Cyber Risk Leader
Mobile: +27 83 634 4445
Email: skanjee@deloitte.co.za

Tiaan van Schalkwyk
Risk Advisory Africa:
Mobile: +27 83 475 3551
Email: tvanschalkwyk@deloitte.co.za

Deena Chetty
Risk Advisory Africa:
Mobile: +27 83 452 8509
Email: dchetty@deloitte.co.za

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

Urvi Patel
Director: Risk Advisory East Africa
Mobile: +254 71 405 6887
Email: ubpatel@deloitte.co.ke

West Africa

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +263 867 700 0261
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory Central Africa
Mobile: +263 867 700 0261
Email: rdean@deloitte.co.zm

Deloitte.