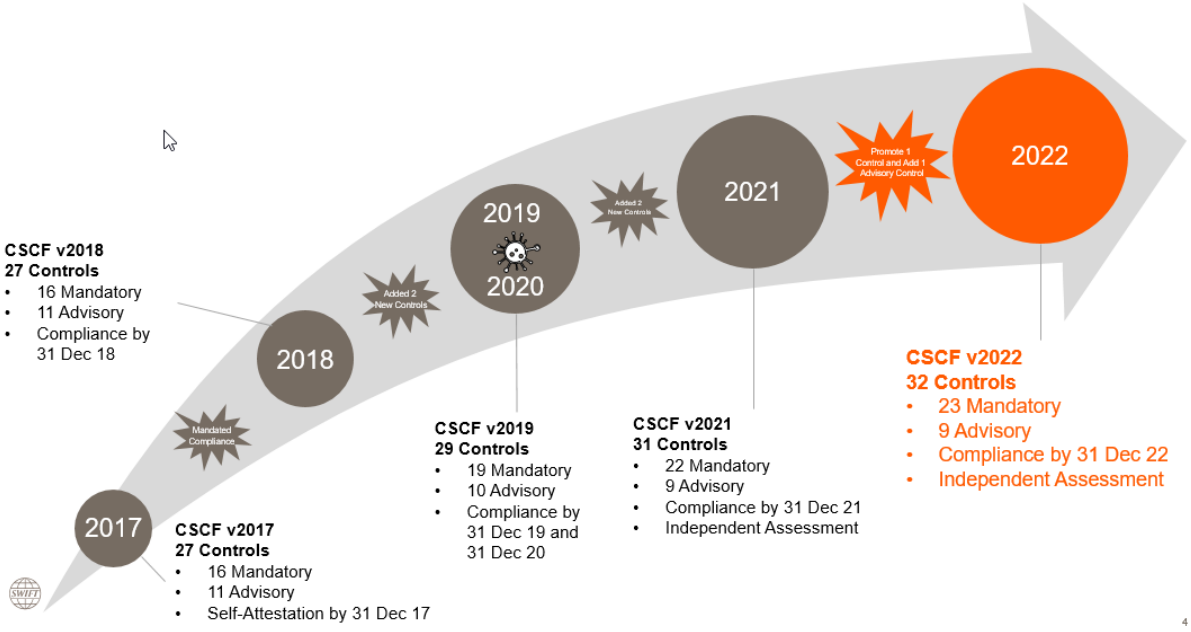
The global provider
of secure financial messaging services

Dear KYC-SA submitter/approver,

SWIFT announces updates to the Customer Security Controls Framework (CSCF) for attestation in 2022

SWIFT has published the updated CSCF v2022, against which customers will need to attest in the second half of 2022. You can access the **CSCF v2022 here**. (SWIFT login ID required).

The updates are the result of extensive collaboration with our community, in line with how the CSP continues to develop overall. The CSCF Working Group centralised, prioritised and reviewed all feedback from the community before finalising the changes summarised below.



Controls: new and updated

Control 2.9 (Transaction Business Controls): Building incrementally on last year's version (CSCF v2021), CSCF v2022 promotes Control 2.9 to mandatory, after clarification of the scope and the existing implementation guidelines. This supports and aligns with other regulations such as the Committee on Payments and Market Infrastructures' (CPMI's) strategy, also aimed at reducing the risk of payment fraud related to endpoint security. It also recognises the effectiveness of such a control in reducing fraudulent financial losses within the community.

Control 1.5A (Customer Environment Protection): This new advisory control is created to ensure protection for the 'customer connector' and other customer-related equipment. It can be achieved by aligning the new control applicable for architecture A4 with the existing control 1.1 already applicable to the other architecture A types.

Control 6.2 (Software Integrity) and 6.3 (Database Integrity): CSCF v2021 introduced customer connectors as an advisory component in scope of numerous controls, which is now established. In addition, to further align with the other

architecture A types, control 6.2 (Software Integrity) and 6.3 (Database Integrity) are set as advisory for architecture A4.

Control 1.2 (Operating System Privileged Account Control): The scope of the existing control 1.2 is extended, on an advisory basis, to general-purpose operator PCs and as such to architecture B. This is to provide basic security hygiene on end-user devices.

As a result, CSCF v2022 now comprises of 23 mandatory and nine advisory controls.

Further minor clarifications or changes have been made to specific controls or to the overall CSCF framework. This is to improve the usability and comprehension of the document and help you implement the framework as intended.

In addition to clarifying on existing controls, you can also consult CSCF v2022 at this point to help you plan and budget for any action required at your end. CSCF v2022 will become effective in KYC-SA, the online repository for customer security attestations, in July 2022.

In summary, attesting compliance against the CSCF v2022 will be mandatory as of July 2022, with a deadline for completion of end 2022. We look forward to continuing to collaborate with our community to help strengthen each user's cybersecurity infrastructure. Working together we can bring more transparency and greater security into the financial ecosystem.

SWIFT announces updates to the Independent Assessment Framework (IAF)

Due to the Covid-19 pandemic, the official launch of the IAF was

put back from 2020 to 2021. We would like to remind the community to start preparing for undertaking an independent assessment before the year-end deadline of 31 December 2021.

The **new version of the IAF** aims to bring further clarification on the following topics:

- Duration of validity of an independent assessment and conditions when a delta (i.e. incremental) assessment needs to be performed to complement an earlier assessment
- Conditions for users to support their attestation without an independent assessment and the impacts of doing so
- Options for users of a Non-SWIFT User Group, such as a service bureau, in terms of attestation and independent assessment
- Certifications required for assessors
- Options for combining internal and external staff as assessors
- Roles and responsibilities in the context of attestation and independent assessment when engaging with a third party

We have compiled a short anonymous survey to help us better understand readiness for IAF implementation among the SWIFT community. This will enable us to provide further support as required.

If you have not done so yet, we would appreciate you giving two to three minutes of your time to **complete the survey**. Thank you in advance for your input.

SWIFT publishes the CSP High Level Test Plan Guidelines (v2021)

SWIFT has published the CSP **High Level Test Plan Guidelines** with the goal of helping SWIFT users and their assessors to carry out their respective independent assessment responsibilities; this document provides a high-level test plan

designed to verify the compliance of the CSP controls (CSCF v2021) with regard to their control definition. Users and their assessor(s) can develop a detailed test plan fully consistent with the applicable CSP controls and their actual implementation using this guidance as a starting point.

SWIFT announces updates to the Customer Security Programme Controls Policy

In early July, SWIFT published the following updates to the **CSP Controls Policy**:

- Option for users to combine external and internal resources to conduct an independent assessment
- Introduction of the option for SWIFT to inform a user's service provider(s) as to whether that user still needs to submit an attestation
- Extension of the definition of non-compliance; namely the submission of an attestation without independent assessment and of the subsequent reporting
- Clarification of the monthly notification sent to customers of the re/de listing of the service bureau serving them

Yours faithfully,

Frank Versmessen
Head of Customer Security | CSP Programme Director

Was this email valuable for you?

Stay connected

Secure mailing practices

Mail sender and embedded links can easily be spoofed. Therefore, mails from SWIFT are always digitally signed and as a receiver, you need to verify the signature. In rare circumstances, our emails may contain embedded links. You must check that:

- Access to SWIFT's website is visible in your browser address bar,
- It uses secure HTTPS protocol, and
- A valid certificate is assigned to SWIFT's website.

SWIFT will never ask you to change your credentials by email, unless you requested a change yourself.