Having difficulties viewing this email? **Click here**

Customer Security Programme Updates

Reinforcing the security of the global banking system

May 2021

Welcome to the SWIFT Customer Security Programme (CSP) update – providing you with the latest information on the security programme.

What's new in CSCF v2021?

In early July, the **Customer Security Controls Framework (CSCF) v2021** will be loaded in the **KYC-SA application**. All customers are required to attest against this version between July and December 2021, with a deadline of 31 December 2021.

CSCF v2021 introduces the following changes:

- Introduction of the new architecture type A4 (aka Customer connectors). These represent a non-SWIFT footprint. They include off-the-shelf products (e.g. file transfer solutions, middleware/MQ servers etc.) or home-made products (e.g. APIs)

- ‘Internet Access’ related provisions have been transferred from control 1.1 (SWIFT Environment Protection) to control 1.4 (Restrict Internet Access).
- In comparison to the CSCF v2019, Controls 1.3 (Virtualization platform) and Control 2.10 Application (Hardening platform) have become mandatory.
- On top of these changes, the CSCF v2021 brings many clarifications, so aiding efficiency and the practical application of controls (e.g. coverage of cloud providers as Third Party).
- Details of changes are (i) highlighted in the tracked change versions of the CSCF available on SWIFT.com in **the Knowledge centre** and (ii) in the **KC article 5024202**, which contains related webinar recordings and slides.

Independent assessment required by end 2021

As per the **Independent Assessment Framework (IAF)**, all attestations submitted between July and December have to be supported by an internal or external independent assessment, with a deadline of 31 December 2021.

Important note: The absence of confirmation of independent assessment in the KYC-SA application will render an attestation non-compliant. It can lead to being reported to supervisors, and the non-compliant status will also be visible to counterparties.

Read the communication about IAF on swift.com to understand the background, the process to follow and the resources offered by SWIFT.

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. We would appreciate you giving two to three minutes of your time to complete the survey Thank you in advance for your input.

Take the survey

KYC-SA new features coming soon

In addition to the introduction of CSCF v2021 and the IAF requirements, the following enhancements will be rolled out in early July:

- Changes when editing your security attestation:
    - You will be able to share the Security Operations Centre (SOC) and Payment Operations (POC) contacts with your counterparties.
    - A new ‘Copy from’ function will allow you to replicate the same contact details to different sections.
    - If you opt for an external assessment, you will be able to select your assessor from a dropdown list.

- Control reports v3 (available for KYC-SA Security Officers)
    - In addition to the new CSCF v2021 controls, v3 will also include other data points from the security attestation to facilitate KYC-SA data consumption.
    - A new ‘Controls compliance status’ will be added for each security attestation you publish or have access to.

- UX revamp underway
    - The KYC-SA will undergo a UX revamp starting with a refresh of the ‘My Entities’ and ‘My Counterparties’ views. Stay tuned!

Migration from STIX/TAXII to MISP – Improved threat intelligence

In addition to the SWIFT ISAC portal, SWIFT has been sharing Indicators of Compromise (IoCs) via an automated feed in STIX format over TAXII protocol. As mentioned in our previous newsletter, the sharing mechanism was migrated to MISP on 18 February 2021. Originally named Malware Information Sharing Platform, MISP is a free, open source threat intelligence platform.

The old STIX/TAXII solution will be decommissioned on 1 July 2021. Please be sure to migrate to the new service in a timely manner, to ensure continuous access to the published IoCs.

Learn more about the MISP migration and how to get the most out of MISP from our FAQ bulletin, including a user guide on MISP. You can access these documents on the **SWIFT ISAC portal**.

Supervisors can request access to the security attestation of their supervised entities

Supervisors, through the KYC Security Attestation for Supervisors (KYS) application, have had the ability to request access to the security attestation data of their supervised entities since Q4 2020. You will see the access requests on the KYC-SA application. The KYS and KYC-SA applications facilitate secure distribution and sharing of attestation data with your counterparties and supervisors.

Mutual sharing of attestation data with counterparties and supervisors leads to increased transparency and cyber hygiene in the financial ecosystem and better cyber risk management.

Please note: All access requests received from a supervisor are tagged with the supervisor label. Information about the access granted to supervisors is only available in the inbox in the KYC Security Attestation application.

Updated cybersecurity toolbox from Carnegie now available – free to use

We have partnered with a range of industry leaders to unite and collaborate in making cybersecurity more accessible. These include the Carnegie Endowment for International Peace and the World Economic Forum. The SWIFT Institute issued Carnegie with a grant to develop a cybersecurity tool box.

Originally released in 2019, this now provides financial institutions with eight easy-to-use guides. These begin at board and executive level to ensure comprehensive risk management, governance and continuous organisational thinking on cyber security. The tool box also outlines actions that CISOs and other security personnel can take to protect customers and critical assets.

Carnegie has continued to develop and improve the toolbox, updating sections and translating it into nine additional languages. Today, it is available in English, Mandarin, Japanese, Russian, Hindi, Spanish, Portuguese, Dutch, French and Arabic.

Download the toolbox from the SWIFT Institute ›

Learn more on www.swift.com ›

UPCOMING EVENTS

Free webinar series: Compliance in an ever-changing world

Since the start of the pandemic, compliance teams have been forced to navigate an ever-evolving risk landscape. While under increased pressure to speed payments up and remove compliance delays, teams must also keep pace with growing customer expectations.

Throughout June and July, we're hosting a series of free webinars that will unpack what these changes mean for our industry. They'll explore:

- ✓ The impact of the pandemic on compliance
- ✓ Building trust within correspondent banking while managing global risk
- ✓ Reducing compliance friction to enable faster cross-border payments
- ✓ Driving compliance forward: The importance of effective collaboration
- ✓ Our bold new strategy
- ✓ How we're supporting the community today, and what our vision of the future looks like

Sessions will be run in English, Spanish and French and are **free** for registered banks and financial institutions with a live BIC8.

Register now

Stay connected

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

You are receiving this update because you have been granted the Admin or Submitter role in KYC-SA in mySWIFT. If you are no longer the right contact person for KYC-SA, you need to contact your Administrator in KYC-SA to remove you from this mailing list. If this edition is relevant, please pass it onto security practitioners in your organization.