Customer Security Programme Updates

Reinforcing the security of the global banking system

October 2019

Welcome to the SWIFT Customer Security Programme (CSP) update – designed to provide you with the latest important information and updates relating to the CSP.

Deadline to re-attest coming up

The deadline to re-attest against the Customer Security Controls Framework (CSCF) v2019 is **31 December 2019**, by which time all SWIFT users must self-attest compliance with the mandatory controls set out in the 2019 version of the CSCF.

Once your self-attestation data has been submitted, SWIFT will publish your submission securely, which can then be consulted on by other customers and used in their counterparty risk management processes.

The presence of the self-attestation and its validity will be visible to all KYC-SA users, but the contents will not be shared without the owner's explicit permission.

The KYC Security Attestation (KYC-SA) application for CSCF v2019 became available on 4 July 2019 and customers should attest their level of compliance against this baseline using this tool.* The CSCF v2019 is available here (SWIFT login ID required).

**If you have submitted an attestation (to SWIFT or to your approver) before or on 4 July 2019, then you have attested against CSCF v2018 and must re-attest against v2019 (and the new mandatory controls set out there) before 31 December 2019. You can do so by editing your current attestation; the new version will then automatically be loaded into the tool.*

How to check against which version of the CSCF you have attested:

As a submitter/approver, go to the bottom of your attestation and verify the baseline that was used. If it says anything other than 'Using baseline 2019.x', then you have not yet attested against v2019.

CSCF v2020

SWIFT has now published CSCF v2020 (which customers will need to self-attest against from July 2020). Under v2020, a number of changes are introduced to the existing controls, along with additional guidance and clarification provided on the implementation guidelines. You can access CSCF v2020 here. (SWIFT login ID required).

Changes outlined in the CSCF v2020, include:

- the promotion of two existing advisory controls to mandatory;
- the introduction of two new advisory controls;
- the extension of an advisory control (2.4A) to include middleware/MQ servers

As a result, CSCF v2020 is now comprised of 21 mandatory and 10 advisory controls. The two advisory controls that have been promoted to mandatory are 1.3 (Virtualisation Platform Protection) and 2.10 (Application Hardening), which aim to protect and reduce potential vulnerabilities on critical systems where virtualisation is being used more frequently, and on critical interface components.

The two new advisory controls that have been introduced are 1.4A (Restriction of Internet Access) and 2.11A (RMA Business Controls).

Furthermore, advisory control 2.4A Back Office Data Flow Security has been expanded to include middleware/MQ servers to help protect the upstream back-office application flows.

Additional controls guidance and/or clarifications have been included in numerous areas, including controls scope, architecture types, security controls compliance, expectations on general operator PCs, token management and intrusion detection.

In addition to clarifications on existing controls, CSCF v2020 should already be consulted to help customers plan and budget any action required on their end. CSCF v2020 compliance data will be available in the KYC-SA application, the online repository for customer security attestations, in July 2020.

As above, self-attesting compliance against the CSCF v2020 will be mandatory as of July 2020 and should be completed (alongside the mandatory independent assessment – see below) by the end of 2020.

New Customer Security Controls Policy published

ISWIFT has updated its Customer Security Controls Policy, which sets out SWIFT's policy with regards to the Customer

Security Controls Framework (CSCF).

The refreshed policy includes the following changes:

- Annual self-attestation window, between July and December
- As of CSCF v2019, self-attestations submitted between July and December will be valid until the end of the following year (replacing the current 12 months validity rule)
- As of mid-2020, an independent assessment (either internal or external) will be required to underpin an attestation as outlined in the recently published Independent Assessment Framework, which is available to SWIFT users here (SWIFT login ID required)
- Policy and CSCF updates will follow an annual joint update cycle
- Elements specific to the usage of the KYC-SA application have been moved from the CSP Policy to the KYC-SA user guide

---

Alliance suite Release 7.2 reaching end of support

When Alliance release 7.2 was released in 2017, its end-of-support date was January 2020. As per SWIFTNet and Alliance release policy, SWIFT has not provided security

updates for release 7.2 since mid-2019. In order to meet CSCF control 2.2, beyond 31 January 2020 an upgrade of all Alliance 7.2 products is mandatory.

This applies to Alliance Access, Alliance Entry, Alliance Gateway, Alliance Web Platform Server-Embedded and SWIFTNet Link.

Alliance suite Release 7.4

With every release of the Alliance product suite, SWIFT improves the underlying security infrastructure. In order to benefit from the highest possible security and most advanced set of features that help you to secure your environment, it is recommended to deploy release 7.4. Release 7.3 reaches end-of-support at the end of April 2021, so customers will have to upgrade to release 7.4 or higher by that date. Release 7.5 will be available in July 2020.

This applies to Alliance Access, Alliance Entry, Alliance Gateway, Alliance Web Platform Server-Embedded and SWIFTNet Link

---

Sibos 2019

With more than 11,000 delegates, 600 speakers and 300 exhibitors, Sibos 2019 London was the largest and most ambitious Sibos to date.
There was a host of fascinating speakers and sessions on cyber, but the moral of the story remains clear – security is the bedrock for every institution, and firms must do everything in their power to prevent, detect and secure.

Have a look here for more on what we talked about at Sibos.

CSP wins top cybersecurity award

SWIFT was recently named best cybersecurity provider in recognition of the CSP at Central Banking's annual FinTech & RegTech Global Awards. The awards ceremony, which took place in Singapore, celebrates the most important and ground-breaking projects that are being undertaken in the community.

With the CSP, SWIFT is reinforcing the security of the entire global banking system. As attackers prove increasingly determined, patient and cunning, breaching local bank systems that once appeared impenetrable, SWIFT has assisted institutions to step up to the growing threat and its programme is delivering tangible results.

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.
