July 2020

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

KYC-Security Attestation application (KYC-SA) upgraded to baseline v2019.3 for attestation in 2020

All SWIFT customers must re-attest compliance with the mandatory controls set out in baseline 2019.3 between July and 31 December 2020. As previously communicated to the SWIFT community, SWIFT has re-phased originally published timelines for the CSCF to make sure upcoming reinforcements are practical for our community. Therefore, you must attest against CSCF v2019 (baseline 2019.3) by the end of 2020.

What is new in baseline 2019.3?

Baseline v2019.3 does not introduce any new controls; it only

brings minimal changes that are listed in the baseline 2019.3 documentation.

How to check against which version of the baseline you have attested or created a draft?

As a submitter/approver, go to the bottom of your attestation and verify the baseline that was used. More details in Tip 5023980.

From now on, you will no longer be able to submit attestations against an outdated baseline.

As the published CSCF v2020 and v2021 contain clarifications on the controls, SWIFT recommends making use of these additional guidelines and clarifications when re-attesting against baseline v2019.3.

Once your attestation data has been submitted, SWIFT will publish your submission securely, which can then be viewed by other customers that have been granted access and used in their counterparty risk management processes.
The presence of the 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.

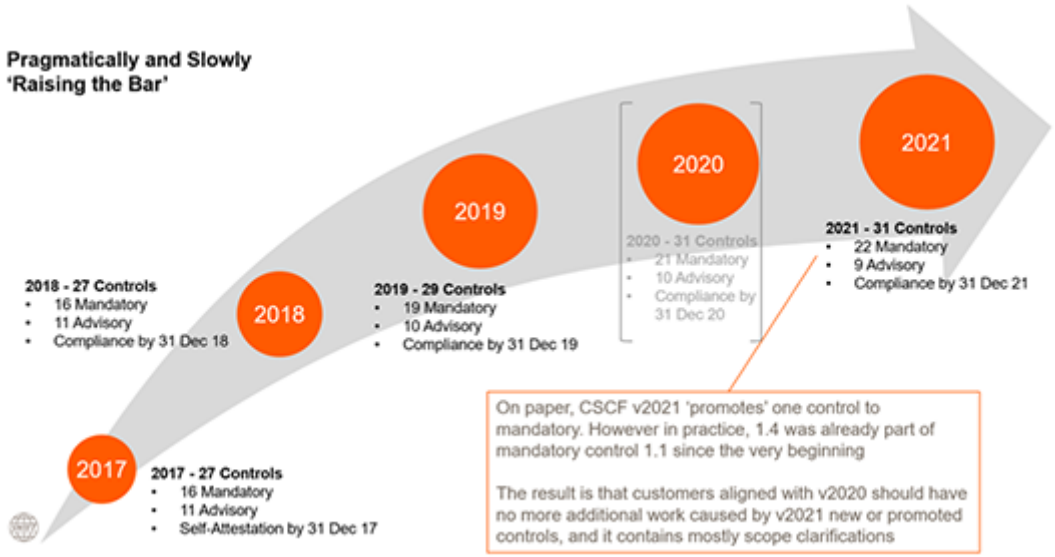
More dedicated CSP information and reviewed FAQs can be found on the security attestation support page on mySWIFT.

SWIFT announces updates to the Customer Security Controls Framework (CSCF) for attestation in 2021

SWIFT has published the updated CSCF v2021 (which customers will need to attest against in the second half of 2021). You can access the CSCF v2021 here. (SWIFT login ID required)

As previously communicated to the SWIFT community, SWIFT has re-phased originally published timelines for the CSCF to make sure they are practical for our community in the light of the pandemic:

Controls previously articulated in CSCF v2020 are combined into CSCF v2021 and changes in CSCF v2021 have been kept to a minimum compared to CSCF v2020.



Compared with the CSCF v2019, the CSCF v2020 promoted two advisory controls to mandatory (1.3 and 2.10) and introduced two new advisory controls (1.4A and 2.11A). In addition, the scope of the CSCF v2020, advisory to start with, extended to middleware servers.

On paper, CSCF v2021 'promotes' one control to mandatory. However, in practice, control '1.4 - Restrict Internet Access', was already part of mandatory control '1.1 - Environment Protection / Network Segregation' since the launch of the original controls in 2017 and aims to control/protect internet access from operator PCs and systems within the secure zone.

As a result, CSCF v2021 is now comprised of 22 mandatory and 9 advisory controls.

In addition, a number of guidelines and scope definitions (mainly for 'connectors') have been clarified to better support attestations and assessments. Also, a new architecture type, identified as A4,

which covers customers with non-SWIFT footprint, has been introduced. Its introduction will be able to support new technology usage such as cloud and APIs and paves the way for the future.

Further clarifications have been made to help you implement the framework as intended and highlight expectations on the usual initial cyber targets: the general operator PCs connecting to local or remote infrastructure. Some of the community suggested implementations have also been incorporated (for instance in control 1.1, 2.9A and 6.1)

To enhance efficiency and ensure continuous identification of components in the controls' scope, an initial list is proposed in Appendix F. This list will be regularly updated online.

In addition to clarifications on existing controls, CSCF v2021 should already be consulted to help you plan and budget for any action you are required to carry out. CSCF v2021 will become effective in KYC-SA, the online repository for customer security attestations, in July 2021.

In summary, attesting compliance against the combined CSCF v2020 / v2021 controls will be mandatory as of July 2021 and must be completed by the end of 2021.

SWIFT announces updates to the Independent Assessment Framework (IAF)

SWIFT has published a revised version of the Independent Assessment Framework (IAF).

As previously communicated to the SWIFT community, SWIFT has aligned the introduction of the mandated Community-Standard Assessments with the combined CSCF v2020 / v2021 controls, **with a start date of July 2021 and a deadline of**

December 2021. Subsequently, the option to select the self-assessment option as ‘Assurance type’ in KYC-SA remains available, along with the independent internal or external assessment options. In addition, SWIFT Mandated External Assessments will still be requested in 2020, but will have to be performed by the end of 2021 against the CSCF v2021.

Other significant updates to the IAF include: (i) the definition of reasonable comfort that assessors should seek and (ii) some guidance regarding the performance of remote assessment.

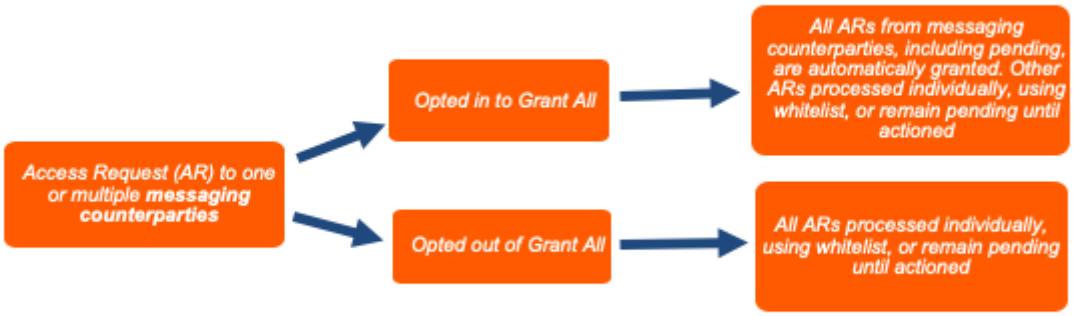
KYC-SA Grant All Features and Functions

Customer Counterparty attestation data is a key input to overall cyber risk management processes. In order to achieve an increase in consultation and consumption of counterparty attestation data with enhanced operational efficiency amongst all institutions, SWIFT will introduce a ‘grant all’ function on the KYC-SA. This will provide a functionality to automatically grant attestation data access requests (ARs) received from existing messaging correspondents. Currently, ARs remain pending until they are processed individually, or granted using the whitelist function.

Implementation of Grant All

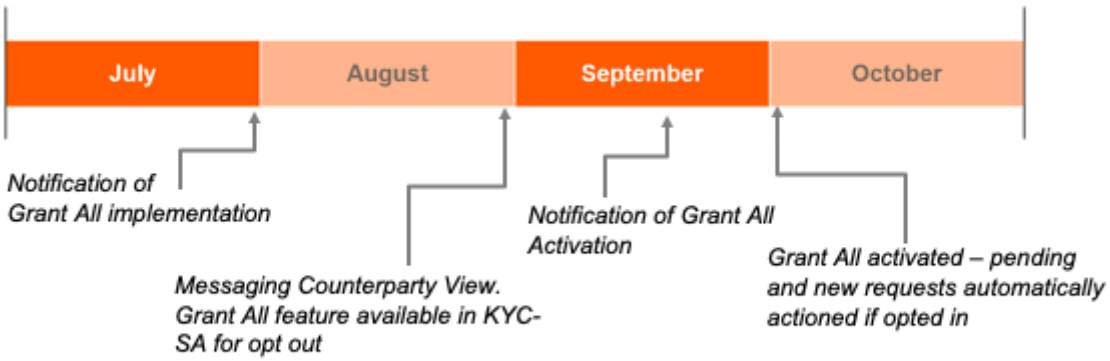
For customers with large numbers of counterparties, to make the Access Request (AR) process easier to manage for counterparty risk management, a ‘Grant-All’ feature is being implemented, per ER 1204 that was approved in March 2020. Grant All will be implemented in two stages - during the first stage, institutions will be able to opt out of Grant All before it is activated in early October, and new ARs are granted. On activation of Grant All, the second stage will see automatic processing of ARs from messaging counterparties for all institutions which remain opted in. The two implementation stages are planned as follows:

- An enhanced messaging counterparty view will become available on the KYC-SA in August so that users can review their counterparty list along with an opt-out toggle. KYC-SA Security Officers of those institutions who wish to opt-out may do so when Grant All becomes available. By default, all institutions are opted in to Grant All, and can decide to opt out of the function at any stage
- In early October, Grant All will be activated. If you decide to opt out of Grant All before activation, there will be no impact on how you handle the ARs you receive, and you should continue to check regularly for new ARs, and process them in a timely manner. All received access requests will be granted for those users that did not opt out as per the first part of the flow diagram below



Communication

The exact availability and activation dates, as well as related documentation, will be provided in a communication in late July followed by an activation notice in early September.



Migration from STIX/TAXII to MISP

In addition to the SWIFT ISAC portal, SWIFT has been sharing Indicators of Compromise (IoC) via an automated feed in STIX format over TAXII protocol. In a constant effort to improve our offering, we are planning to migrate the sharing mechanism to MISP and decommission the current STIX/TAXII solution in the coming months. We will plan for a migration period allowing you to adapt and keep on receiving the published IoCs. More information will follow in the coming weeks via the SWIFT ISAC portal.

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.
