Action required: Independent assessment of security attestation due in December 2021

Dear KYC-SA submitter/approver,

Participants in the Customer Security Programme (CSP) have eight months to support their KYC security attestation with an independent assessment. Below we have provided background to this requirement, the process to follow and resources offered by SWIFT.

Background

In 2018, SWIFT's board requested that SWIFT implement a mechanism to further improve the consistency of security attestations. The end goal is to ensure the veracity of overall attestation results for optimised counterparty risk management.

SWIFT established the '*Independent Assessment Framework* *(IAF)'.* The aim is to for all KYC-SA attestations to be confirmed through an assessment by one of the following:

- Internal independent assessors: second or third line of defence or its functional equivalent
- External assessor
- Mixed assessor teams composed of internal and external staff

Participants can start planning as soon as possible around the resources required to conduct their independent assessment. This is so that by 31 December 2021 at the latest, each can reflect its conclusions in their attestation.

Benefits

The provision of independent assessment brings benefits to the SWIFT community in the following ways:

- **Greater trust:** It ensures the independence of the assessment supporting an attestation, strengthening trust in the attestation between counterparties and with supervisors.
- **Improved security:** Skilled and expert assessment staff can independently confirm the implementation of a sound security framework, mapped to internationally recognised security standards, ultimately raising the overall security position of the SWIFT community.
- **Enhanced risk management:** It supports informed risk management decisions.
- **Manageable costs:** It provides a way to assess each user's security position at a reasonable cost.

Core requirement

Customers are required to attest in the KYC-SA application between July and December 2021. Within the attestation, customers will also need to provide details of their chosen type of assessment and some reference details.

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

SWIFT resource: Watch a video emphasising the importance and benefits of independent assessment.

Managing costs

In working to reduce the cost of an assessment, it is useful to think about the following:

- The IAF mandates an assessment, not necessarily an audit.
- Consider the merits of internal versus external resources, or a mixed team.
- Consider switching between internal and external resources.
- Use a risk-based approach to assess the controls.

- Ensure accurate scope: consider in-scope components only and do not assess items not in scope (e.g. back office).
- Use the CSP Decision tree to identify an organisation's CSP architecture type.
- Do not assess all components of the same category (e.g. all General Purpose Operator PCs); apply sampling of identical components wisely.
- Leverage previous relevant and current (i.e. no more than two years old) assessment results/documents.
- Make sure that at minimum, the lead assessor has the relevant certifications (international or comparable local certifications), and closely oversees other team members who may not have all appropriate certifications. Note that experienced internal audit staff typically already have the relevant certification.
- Compare multiple assessors' quotes.
- Consider automated compliance verification and reporting and/or continuous monitoring.
- Consider engaging with a service provider (e.g. SIP/L2BA) to conduct the assessment.

Resources

Knowledge Centre (SWIFT.com credentials are required): To increase familiarity with the IAF, we recommend that CSP participants and their assessors use the following documents in the centre:

- **Independent Assessment Process guidelines**: supporting assessors for a streamlined assessment process.
- **The Independent Assessment Framework**, including the CSP curriculum (Annex A of the IAF).
- **FAQ article 5022902**: complementary to the IAF, with translations in major European and Asian languages available.
- **Recommended assessor templates (Excel)**: assessors can use them to (i) read and assess the controls in a logical manner by answering closed ended questions against each control and (ii) to easily document their conclusions and gaps and share them with customers.
- **Recommended completion letter (Word)**: assessors can confirm completion of their assessment in this letter. Please note, SWIFT reserves the right to request a copy of this letter.
- **Recommended controls matrix (Excel):** to assist customers and assessors in determining the elements in scope per security control as a function of the CSP architecture type.
- **CSP Decision tree**: to assist in determining the CSP architecture type.
- SWIFT Products Security guidance: for mapping with the security controls.

Further help and support

The following many also be useful in learning about and obtaining support on the IAF or the CSP more generally:

- CSP Support page: hub of all CSP Information.
- MySWIFT: a self-service portal containing 'how-to' videos, guidance on frequently asked questions and Knowledge Base articles.
- SWIFT Support Centres (24/7)
- SWIFT Professional services
- Training
  - SWIFTSmart training modules (covering the IAF and CSCF controls)
  - The SWIFT Assessment Guidelines workshop (chargeable)
- Directories
  - CSP Assessors/ Cybersecurity providers

We hope this information is useful in working to meet the December 2021 deadline for independent assessment.

Please contact Support for any questions you might have. Do not reply to this email address, it is not monitored.

Yours faithfully,

Frank Versmessen
Acting Head of Customer Security | CSP Programme Director