Customer Security Programme Updates

Reinforcing the security of the global banking system

January 2021

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

Attestation rate for 2020 now available

We're grateful to our community for their work in attesting to their compliance with the CSP's Customer Security Controls Framework (CSCF). This has resulted in a solid attestation rate for 2020.

- For the 2020 year-end CSP deadline the overall attestation rate was 89%
- The attested BICs are responsible for sending over 99% of all FIN traffic on SWIFT
- The average compliance rate for each individual mandatory control ranged from 93% to 99%

The programme is delivering tangible results as the annualised figure for funds targeted by attackers dropped by a factor of three in 2020 compared to 2016, and we now recover the vast majority of funds targeted by attackers. That said, this journey will never be over, so it's vital that all customers continue to work closely with SWIFT as we strengthen our cyber defences further.

Learn more about attestation in 2020 and requirements for customers in 2021 in our latest article on swift.com.

Independent assessment required by end 2021

The Covid-19 pandemic led to a revision of the previously announced schedule for mandatory independent assessment, with timings re-phased from 2020 to 2021. Customers are now required to back their attestation with an external or internal independent assessment by the end of 2021.

Assessment not audit: This request is limited to an assessment and not an audit, so there is less cost, effort and time involved. The assessment can be carried out by internal or external resources, or a mixed team. An internal independent assessor is typically the second or third line of defence (e.g. risk office or internal audit respectively) or their functional equivalent within a company. If an external party, you can select one from the list of CSP assessors published on swift.com.

Managing costs: To contain costs we advise you to consider the following:

- Remember that this is an assessment, not an audit
- Ensure an accurate scope for the assessment
- Identify the correct architecture type
- Only consider in-scope components

- Apply sampling of components wisely
- Consider internal vs. external resources or even mixed team
- Leverage previous relevant and current assessments
- Consider implementing supervisory controls (i.e. methods confirming the control compliance in an automated way) and continuous monitoring
- Consider using one of your service providers (e.g. SIP/L2BA) to conduct the assessment

Find out about remote assessments: We're also mindful that the ongoing Covid-19 pandemic may limit the ability to travel and conduct an on-site assessment. For guidance and supporting materials on remote assessments see section '6.1 Potential Assessment Methods' within the Independent Assessment Framework (IAF) section on swift.com.

Access educational resources on the IAF: You can learn more about independent assessments, including the difference between assessment and audit, on SWIFTSmart.com. Log in or register to access the module 'Independent Assessment Framework v2021'.

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

In Q4 2020, SWIFT deployed new functionality allowing local supervisors to request access to attestation and control-level details for their supervised entities. Supervisors, through the KYC Security Attestation for Supervisors (KYS) application, can now request access to the security attestation data of their supervised entities.

Sharing attestation data is a key aspect of cyber risk management. Through the KYS, SWIFT aims to simplify sharing this information with the supervisor community.

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.

Migration from STIX/TAXII to MISP – Improved threat intelligence

As part of supporting our community in strengthening its cyber defenses, we're migrating the SWIFT ISAC automated threat intelligence feed (currently STIX/TAXII feed) to MISP. Originally named Malware Information Sharing Platform, MISP is a free, open source threat intelligence platform.

MISP brings benefits including the ability to fetch data in multiple formats. Meanwhile, MISP sync enables the synchronisation of threat events between servers for an automatic threat feed.
The new MISP solution went live for all CSP participants on 18 February. The SWIFT ISAC portal remains as is and will continue to be updated with human readable reports.
Users of the existing STIX/TAXII solution have until the end of June 2021 to migrate to MISP. The migration period will provide time to adapt and allow customers to continue receiving published indicators of compromise via the STIX/TAXII feed.

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.

SWIFT at SIBOS – Cybersecurity session – 9 March 2021

Our cybersecurity sessions during SIBOS 2020 week had record-breaking viewership. The SIBOS digital monthly series follows, running November 2020-March 2021. Join us for our last session: Bringing Cybersecurity to the Masses – Does the Answer Lie in New Tech?

It takes place on **Tuesday, 9 March 2021, broadcast from 11am CET.**

Speakers include:

- **Ms Sharon Barber,** Chief Security Officer, Lloyds Banking Group
- **Mr Johan Gerber,** Executive VP of Security and Cyber Innovation, MasterCard
- **Ms Lisa Lee,** Chief Security Advisor FSI, Microsoft
- **Mr William Hoffman**, CISO for UK and Ireland, Deutsche Bank
- **Heather McKenzie**, freelance financial journalist, Fintecheye – moderator

Learn more and register for the session ›

Register for free webinars on CSCF and IAF requirements in 2021

During Q1 and Q2 2021, SWIFT will schedule webinars across regions to support customers on requirements in 2021. These webinars will cover:

- A refresher on the CSCF v2021 (contents of the CSCF v2021 and timeline for compliance)
- the IAF (difference between assessment and audit, types of assessments, process, timeline and workflow)

Webinars will be held in English and several other languages.

Register now