1 SWIFT Customer Security Controls Framework

Why has SWIFT launched new security controls?

SWIFT has published a set of baseline security controls that all users must implement on their local SWIFT-related infrastructure. These controls reflect good security practice and should also apply beyond the SWIFT-related infrastructure into the broader end-to-end transaction chain. These controls are intended to help customers to safeguard their local environments and reinforce the security of the global financial community.

What are the main principles?

All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond' (see figure below) which, in turn, are linked to eight security principles and twenty-seven controls. The controls have been developed based on analysis of the latest cyber-threat intelligence and in conjunction with industry experts. The control definitions are also designed to be in line with existing information security industry standards.

Secure your environment

1. Restrict Internet access
2. Segregate critical systems from the general enterprise IT environment
3. Reduce attack surface and known vulnerabilities (for example, by ensuring timely security updates)
4. Physically secure the environment.
Know and limit access

1. Prevent the compromise of credentials
2. Manage identities and segregate the privileges of local infrastructure users.

Detect and respond

1. Detect anomalous activity on systems or transaction records
2. Plan for incident response and share information.

The detailed security controls which support these three overarching security objectives and eight core principles were published in April 2017.

What is the scope of the security controls?

SWIFT’s security controls and related attestation process apply to the SWIFT-related infrastructure of the users. However, SWIFT recommends that these controls are applied into the broader end-to-end transaction chain as a matter of good security practice.

How will the SWIFT Customer Security Controls Framework be rolled-out?

In April SWIFT published the Customer Security Controls Framework, a detailed description of the mandatory and advisory customer security controls providing a security baseline for the community. To encourage adoption, and to complement the Framework, in May, SWIFT published details of the related security attestation policy and self-attestation process in the SWIFT Customer Security Controls Policy document found in the customer security programme section of the user handbook on swift.com. A detailed description of each data field required to complete the self-attestation is available in The KYC Registry Security Attestation Baseline document available on mySWIFT.

SWIFT has now opened The KYC Registry Security Attestation Application (KYC-SA) a central application for users to self-attest their level of compliance with SWIFT’s security controls.

All SWIFT users must log in to the application to submit a self-attestation for each of their live BIC8s before the end of December 2017. Please join the KYC Registry Security Attestation Application upon receipt of the welcome email that will be sent to all swift.com administrators, and submit your self-attestation as soon as practicable. Users can also request through the KYC SA to view the attestation data of their counterparts to support cyber risk management and business decision making.

Will all of the security controls be enforced?

The SWIFT Customer Security Controls Framework comprises 16 mandatory and 11 advisory controls. All users must self-attest compliance against the mandatory controls before end of 2017. Implementation of the advisory controls is strongly recommended to further strengthen the security of users’ local infrastructure.

How have the controls been designed and validated?

The controls have been developed based on analysis of the latest cyber-threat intelligence and in conjunction with industry experts. The control definitions are also designed to be in line with existing information security industry standards.
How do SWIFT’s customer security controls map with international security standards?

The security controls have been mapped against the following 3 international security standards: PCI-DSS, ISO 27002, and NIST. The mapping table is published in the CSCF.

What if a user’s SWIFT technology footprint is limited, do they still need to confirm compliance with the security requirements?

All users must self-attest against the mandatory security controls, irrespective of whether connecting to SWIFT directly or indirectly. The SWIFT Customer Security Controls Framework document describes the different technology footprints and architecture types and indicates the in-scope components.

How can users implement the SWIFT security controls?

Each security control is supported by recommended implementation details, a description of the IT components it relates to as well as suggested optional enhancements. In addition, SWIFT provides a mapping between the security controls and the recommendations from SWIFT security guidance documents (Alliance Security Guidance, Certified customer managed interface, the Alliance Remote gateway, Alliance Lite2). Customers can find this information in Knowledge Base tip 5020786.

2 On the Customer Security Attestation Process

What are the drivers behind self-attestation?

The Customer Security Attestation Process is designed to incentivise genuine improvements in security across the community; it is not a ‘tick-box’ exercise.

The approach fosters transparency between SWIFT users to strengthen security.

The CSAP is designed to remain practical for SWIFT’s customer base of more than 11,000 institutions across 200+ countries, and allow for information sharing between users (which includes over one million counterparty relationships between users).

The CSAP allows for the continuous evolution of SWIFT security controls and is sensitive to the need for users to self-attest compliance to the initial version of the controls and subsequently transition to future versions.

How will the overall process work – is it a one-off exercise?

No it is not a one-off exercise. Attestation will be required at least every 12 months. From a high-level process perspective, the CSAP will be based upon three main steps:

1. **Contribution of attestation information** through which a user attests their level of compliance to SWIFT’s security controls

2. **Publication to other users to enable transparency between SWIFT users** (with each user retaining control to grant access to their own data)

3. **Follow-up activities to drive compliance and improvements in security** (which includes SWIFT reserving the right to inform supervisors or, as the case may be, messaging counterparties about the compliance status of specific users)
Where can I find more in-depth operational information on the self-attestation mechanisms?

SWIFT has published the SWIFT Customer Security Controls Policy document which contains detailed information on:

- The obligation for users to self-attest against SWIFT’s mandatory security controls.
- The process and timelines for submitting self-attestation data to The KYC Registry Security Attestation Application.
- The process for viewing counterparties’ attestation data via the KYC Registry Security Attestation Application.
- Follow-up process in cases of non-compliance.

SWIFT strongly urges customers to consult this document which is available on the User Handbook section of mySwift, and to begin preparation. Additional tools such as the KYC Registry Security Attestation User Guides, How to videos, and SWIFTSmart training and e-learning modules are also available on MySWIFT to help.

When can I submit my self-attestation?

The KYC registry Security Attestation Application is now open for the submission of self-attestation data. All SWIFT users must have submitted a self-attestation by the end of December 2017 and at least every 12 months thereafter. From January 2018 onwards, SWIFT reserves the right to report to supervisors or, as the case may be, messaging counterparties, users that have failed to submit a self-attestation on time.

What can you do to prepare for self-attestation?

- Review and understand the controls, identify any current gaps and prepare how to address them in your organisation.
- Already map your compliance against SWIFT’s existing security guidance documents.
- Assess budget and resource implications for implementing the controls if relevant.
- Ensure you are prepared to meet the attestation timelines. Your first attestation must be submitted in the Security Attestation Application before the end of December 2017.

Please join the KYC Registry Security Attestation Application upon receipt of the welcome email that will be sent to all swift.com administrators, and submit your self-attestation as soon as practicable.

Will SWIFT certify or recommend third party firms to validate users’ compliance?

SWIFT will not introduce an independent third party certification process. Users requiring specific support to assess, remediate and provide assurance against the security controls can engage a third party firm. SWIFT publishes a directory of cyber security service providers for users’ reference only; users may select any service provider they determine is appropriate and there is no requirement to use a provider listed in this directory. The Directory of Cyber Security Service Providers is available on the CSP > Community engagement pages of swift.com. Users must always conduct their own analysis of the suitability of a Cyber Security Service Provider for their own purposes.
How can users self-attest compliance with the mandatory security controls?

The KYC Registry Security Attestation Application is now open for attestation data submission and consumption. Each SWIFT user must assign designated staff to submit and approve its attestation data.

For each security control, users will be able to self-attest by selecting one of the following options:

- I comply as per the implementation guidelines in the SWIFT Customer Security Controls Framework
- I comply using an alternative implementation while meeting the same control objective (with an optional text field to document an explanation)
- I will comply by a given date (with an optional text field to document further explanation). Specifying a later compliance date does not affect SWIFT’s right to report non-compliance
- I do not comply (with an optional text field to document further explanation)
- Not applicable (with an optional text field to document further explanation) this option is limited to specific controls.

It remains each user’s responsibility to submit a correct and complete attestation for all mandatory controls. It is optional to include compliance status information for the advisory controls. Submitters can also highlight if the attestation response has been validated through an internal and/or external audit.

For what period of time does a self-attestation submission remain valid?

Each published data set is valid for a 12-month period starting at the publication date subject to the obligation for users to update relevant changes in circumstances within one month, such as a change of architecture type or service provider or if the information in the self-attestation is no longer accurate, complete, or up-to-date.

When will users’ self-attestation information be made available to others within the attestation platform?

The KYC Registry Security Attestation Application is now open for both data submission and consumption.

How will SWIFT users verify who is registered as their CISO?

The CISO and SOC information will now be captured in the KYC Registry Security Attestation Application and self-managed by the customer.

Are Service Bureaux subject to the CSP?

SWIFT has been engaging with service bureaux that are offering connectivity to SWIFT since 2013 through the Shared Infrastructure Programme (SIP). This programme, which contains legal, financial and operational requirements, includes a formal certification reflecting the service bureau’s compliance at a certain point in time with the then current SIP requirements. The list of certified Service Bureaux is publicly available on swift.com. The security requirements within the Shared Infrastructure Programme are (and will continue to be) aligned with the security controls set out in the SWIFT Customer Security Controls Framework document. The certification programme includes an onsite verification of compliance not less frequent than once every 3 years.
How will customers of Service Bureaux know whether their own Service Bureau is certified?

A Service Bureau that is certified is listed in the Service Bureau directory on swift.com with an indication of the release of the Shared Infrastructure Programme. Service Bureaux can be removed from the directory in case of continued non-compliance issues as set out in the Shared Infrastructure Programme Terms and Conditions. At the time of self-attestation by an individual customer, the certification status of his Service Bureau will also become visible in the attestation application, and it will subsequently be visible to the counterparties of the customer whom the customer decides to give visibility on his own CSP compliance.

Will it be visible in the Security Attestation Application which service bureau a customer uses to connect to SWIFT?

The attesting user will have the option to indicate the name of its service bureau.

At which level must an attestation be submitted? Customer Parent Destination (CPD), BIC, or HUB level (where more than one branch is hosted)?

Each SWIFT user must self-attest for all its live 8-character BICs, regardless of the architecture type. In the case of a group of multiple affiliated users belonging to the same SWIFT traffic aggregation hierarchy, the access to the KYC SA is granted by default through the user heading the traffic aggregation hierarchy. Users wanting to change this default setup must contact SWIFT Customer Support.

Is there a process whereby clients can seek a waiver or commit to a timeline for compliance as part of self-attestation? If not do you suggest another approach?

Users who do not comply with a specific requirement can indicate in their self-attestation by when they will comply (with an optional text field to document further explanation).

Will self-attestation deadlines be flexible if users face budget or resource challenges?

No. All users must self-attest against the mandatory controls in the same time frame.

If a user selects to provide additional assurance via internal audit or third party review, will the results be made available via the KYC Registry Security Attestation Application?

Users will be able to provide information on the type of assessment used for the self-attestation (self-assessment, internal audit and/or external review). In the case of an external audit, the name of the third-party assurance provider must also be specified and will be included in the self-attestation shared with counterparties. Users will not be able to upload any reports on the KYC Registry Security Attestation Application. Possible sharing of audit review documentation should occur on bilateral basis using an alternative channel.

When does a user require internal audit/external reviewer sign-off of the security controls?

Users can choose to conduct an internal audit and/or use an external assurance provider to support their self-attestation. The type of assessment used must be specified and confirmed within the self-attestation. At the time the user fills in the self-attestation, they can indicate specifically if they are supported by a self-assessment and/or Internal audit and/or external review. In the case of an
external audit, the name of the third-party assurance provider must also be specified and will be included in the self-attestation shared with counterparties.

3 On the use of The KYC Registry Security Attestation Application

Why does SWIFT use The KYC Registry to support the attestation process?

The KYC Registry is a readily available sharing platform offered by SWIFT. Via a dedicated Security Attestation Application, users will be able to store their attestation data and share with other selected users. The KYC registry provides an efficient mechanism to share information.

How do you protect data in The KYC Registry Security Attestation Application?

The KYC Registry Security Attestation Application includes technical, physical, and organisational security controls to protect customer data against unauthorised access. SWIFT takes the protection of customers’ data very seriously and regularly carries out intrusion testing exercises to verify the effectiveness of its controls.

Do I have to subscribe to the KYC Registry to be able to self-attest?

No. The KYC Registry Attestation Application is automatically available to all connected live users. You do not have to be a subscriber to SWIFT KYC Registry services to use this application to self-attest.

What self-attestation information will be stored in the KYC Registry Security Attestation Application?

In the Security Attestation Application, the user will complete a standardised set of Security Attestation-related data, called the data baseline.

The data baseline is composed of the following elements:

- Contact details
- Assurance type
- SWIFT infrastructure
- Security Controls compliance details

Who will be authorised to view the self-attestation information in the Security Attestation Application?

The attesting user retains approval authority over access to its attestation data by its counterparties. Any user that wishes to view the attestation of another user must first request the attesting user’s approval to view its data.

Will the attestation information be available to non-SWIFT users?

The KYC Registry Security Attestation Application is for SWIFT users only.

Will SWIFT inform users when the attestation data in the Security Attestation Application for their counterparties is updated?

The KYC Registry includes an alerting mechanism. Users that have been granted access to view the attestation data of a counterparty will be informed of subsequent changes to that attestation.
Do users have to pay to use the Security Attestation Application in order to submit security attestation information?

No. The KYC Registry Security Attestation Application is available at no additional charge.

Which languages does the KYC Registry Security Attestation Application support?

The KYC Registry Security Attestation Application is available in English.

4 Regarding Customer Security Work Sessions

When will the Customer Security Work Sessions commence?

Community engagement Customer Security Work Sessions worldwide commenced in April 2017 and will continue to run through to December 2017.

Are the Customer Security Work Sessions only for the big banks?

No. SWIFT users are invited to attend. Customer Security Work Sessions are developed in close coordination with National Member and User Groups and their networks, and also central banks, corporates, banking and other industry associations as appropriate.

Where can I find out about the Customer Security Work Sessions in my area?

Information on the Customer Security Work Sessions is posted in the Customer Security Programme section on swift.com, and customers are invited to attend. Prior to the Customer Security Work Sessions being conducted in a specific country, SWIFT will reach out to the National Member and User Groups to discuss engagement and practical arrangements for the Customer Security Work Sessions in their country.

What will be presented at the Customer Security Work Sessions?

In terms of content, the Customer Security Work Sessions provide an opportunity to share information on the SWIFT Customer Security Controls Framework and Customer Security Attestation Process, as well as to understand local needs and in some cases to introduce cyber security service providers for users’ reference. SWIFT will also provide the community with direction on how and where to access further updates including self-service tools such as the mySWIFT knowledge base, SWIFTsmart for training, the CSP pages on swift.com and direct channels into local experts. As the Customer Security Work Sessions are rolled out worldwide, we will centrally monitor and collect feedback, providing further updates to Frequently Asked Questions that can be shared back with the community. Customer Security Work Sessions take place between April and December 2017 worldwide.

- end -