Customer Security Programme

SWIFT Customer Security Controls Framework and KYC Registry Security Attestation Application FAQ

1 SWIFT Customer Security Controls Framework

Why has SWIFT issued a set of security controls?

In 2017, SWIFT 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. The 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.

SWIFT Customer Security Controls Framework		
Secure Your Environment	1.	Restrict Internet access
	2.	Protect critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

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.

Are all of the security controls mandatory?

The SWIFT Customer Security Controls Framework (CSCF) comprises 16 mandatory and 11 advisory controls. All users must self-attest compliance against the mandatory controls. 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 existing 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 compliance against the mandatory security controls, irrespective of whether they connect 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.

Will there be changes to the mandatory controls during 2018?

The current version of the Customer Security Controls Framework (v1, published April 2017) will remain effective in 2018. No changes to the control requirements will be put into effect in 2018 unless there are important unexpected developments requiring immediate action and update of the Customer Security Control Framework to optimise strong security within the SWIFT user community.

SWIFT is currently developing a change management model to evolve the Controls Framework in the future which will maximise the time for SWIFT users to understand and implement any future changes to the controls requirements.

Is SWIFT developing a quality assurance framework?

SWIFT's Customer Security Controls Framework and Attestation Process are designed to drive cyber security improvements and transparency across the global financial community. Implementing a quality assurance framework is one of the measures that will be put in place to assure the ongoing quality and effectiveness of the overall framework. SWIFT has identified a set of risk indicators to track the overall effectiveness and quality of the Customer Security Controls Framework and associated activities (i.e. attestation, compliance, consultation). If the risk indicators (either individually or collectively) suggest an underlying problem, SWIFT will evaluate the information, make a formal recommendation, and execute the appropriate corrective actions. Further details will be shared with the community in the coming months.

2 On the Customer Security Attestation Process

What are the drivers behind self-attestation?

The customer security attestation process (CSAP) 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 evolution of SWIFT security controls and is sensitive to the need for users to self-attest compliance against the current version of the controls and subsequently transition to future versions.

How many attestations have been published?

We are pleased to report that 89% of the connected and live BIC8s on the SWIFT network attested their level of compliance with the mandatory security controls by the December 31st deadline. Combined, these institutions account for over 99% of all FIN messages sent over the SWIFT network. The number of attestations continues to rise, as users continue to self-attest. If you have not yet attested, you should do so as soon as possible. You can find detailed information and resources on how to attest on the CSP webpages on swift.com – from there you can also log into the KYC-SA tool and complete your submission.

Where can I find more in-depth operational information on the self- attestation process?

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 requesting access to counterparties' attestation data via the KYC Registry Security Attestation Application
- Quality assurance and reporting in case of non-compliance.

SWIFT encourages users to consult this document which is available on the User Handbook section of mySWIFT. 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.

Will SWIFT certify or recommend third-party firms to review users' compliance?

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.

What is the timeframe of the annual attestation cycle? When is the next attestation due?

Users must attest their compliance with all mandatory controls as defined in the Customer Security Controls Framework (v1, published April 2017) by 31 December2018 at the latest.
The Security Attestation Application always indicates the date on which a self-attestation was published. In principle, a published self-attestation is valid for a 12-month period commencing on the publication date. At least every 12 months, a self-attesting user must publish a new self-attestation. The Security Attestation Application is designed to trigger automatic notifications to users prior to the expiry date of a published self-attestation. The attesting user must also submit a new self-attestation if there are other material changes in circumstances, such as a change in architecture type, change in service provider, or a change in the security controls compliance status.

What controls do I have to attest against by the end of 2018?

The priority for 2018 is to confirm compliance with the mandatory security controls. Any gaps you identified when you assessed your compliance with the mandatory controls will need to be closed, and you should re-attest your compliance with all mandatory controls by year-end at the latest. If you require additional support please refer to the CSP materials available via the User Handbook, SWIFTSmart training portfolio, mySWIFT, Knowledge Based Tips, Videos, Webinar recordings, and FAQs. If you require additional support please refer to the CSP materials available via the User Handbook, SWIFTSmart training portfolio, mySWIFT, Knowledge Based Tips, Videos, Webinar recordings, and FAQs.

When is a users' self-attestation information available to others within the attestation platform (KYC-SA)?

As soon as published, a user's attestation status is made available to all parties with access to KYC-SA.

Detailed content of the attestation is available to requesting counterparties that are explicitly authorised by the owner of the attestation.
Users should incorporate the assessment of counterparties' attestation data into their risk management and business decision-making processes – alongside other risk considerations such as KYC, sanctions and AML. Using the KYC Registry Security Attestation Application (KYC-SA), users can share their attestation data with their counterparties and request data from others. This creates an opportunity for your organisation to be transparent about your compliance status, which may increase the trust and confidence of your counterparts in doing business with you.
The transparency provided by this counterparty data exchange system is driving attestation and compliance with the controls, as institutions seek to demonstrate their cyber security to their counterparties. You control access to your attestation – you can grant or deny requests to view your attestation.

How can users verify who is registered as their CISO or SOC?

The CISO and SOC information is captured in the KYC Registry Security Attestation Application (KYC-SA) and self-managed by the user directly.

Are Service Bureaux subject to the CSP?

The Shared Infrastructure Programme (SIP) is designed to establish and maintain a high level of security and resilience for Service Bureaux operations through a certification model verifying compliance against the SIP requirements at the time of the assessment. The list of certified Service Bureaux is publicly available on swift.com.

To maintain their certification, Service Bureaux have to comply on a yearly basis against the applicable SIP security and operational requirements. In addition, at least once every three years, frequency, determined on risk based parameters, an on-site inspection is performed.

The security requirements within the SIP are aligned with the security controls set out in the SWIFT Customer Security Controls Framework document.

How will Service Bureaux customers know whether their own Service Bureaux is certified?

A Service Bureaux that is certified (or in assessment) is listed in the Service Bureaux directory on swift.com with an indication of the release of the Shared Infrastructure Programme it is certified against. 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.
In addition, at the time of self-attestation by a Service Bureaux user, the certification status of the Service Bureaux will be visible in the attestation application, and it will also be visible to the other users granted access to the self-attestation.

Is the name of the Service Bureau visible to counterparties in the KYC-SA?

The Shared Infrastructure Programme (SIP) certification status of the service bureau is visible in the KYC-SA to those counterparties that have been granted permission to view the attestation. By default the name of the service bureau is also visible

Are Interface providers subject to the CSP?
The Certified Interface Programme is designed to ensure that SWIFT interfaces developed by third-parties meet stringent conformance and security requirements, including a set mandatory and

advisory security requirements which have been adapted from the Customer Security Controls Framework. Interface providers were requested to self-attest their compliance against the security controls by the end of December 2017 to qualify for interim certification and to be listed on the certification registry on swift.com. For an interface provider to qualify for full certification, a customer of their choice has to verify and confirm the interface provider's self-attestation. Interface providers must receive customer confirmation by mid-2018 to obtain full certification. We recommend that customers check the status of their messaging interface provider's certification on swift.com.

At which level must an attestation be submitted? Per BIC, at group or individual user level?

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 users can seek a waiver or postpone 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 the date by which they will comply (with an optional text field to document further explanation). All users have to self-attest compliance against the mandatory controls by 31 December 2018.

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

Users provide information on the type of assessment used for the attestation. At minimum, this will include a Self-Assessment. If they additionally leveraged an independent party to support their assessment, they can highlight an Advisory Review by Internal Audit, an Advisory review by External Audit, an Audit by Internal Auditor or an Audit by External Audit. In the case of leveraging 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 are not asked to upload any reports on the KYC Registry Security Attestation Application. Possible sharing of audit review documentation should occur on a bilateral basis using an alternative channel if appropriate.

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

Users can choose to conduct an internal audit, advisory review and/or use an external assurance provider to support their self-attestation.
Should you leverage an internal or external expert to support your assessment and attestation, you need to indicate this in the "Assessment Type" field in the KYC Registry Security Attestation Application (KYC-SA).

We have not attested yet, and the deadline has passed – what do you recommend?

If you have not yet attested, you should do so as soon as possible. You can find detailed information on the attestation process on the Customer Security Programme (CSP) webpages – from there you can also log into the KYC-SA tool and complete your submission.

We have not attested yet but plan to do so in the coming days? Will I still be reported to my supervisor?

The initial deadline for submitting attestations was 31 December 2017. The reporting to supervisors will include the names and BICs of organisations that had not submitted a valid attestation by that date, but will highlight if they have subsequently done so.

3. On Reporting of non-attested users

What are the consequences if users have not yet attested?

From Q1 2018, SWIFT reserves the right to provide a report to supervisors of users within their jurisdiction who have not attested. Additionally, all users with access to KYC-SA can already do a search to see if one of their counterparties has not attested. In Q3, SWIFT reserves the right to make available a report for users to look up non-attested messaging counterparties, the name of the user concerned, and the related 8-character BIC. This will only include their attestation status, not content.

When will SWIFT start reporting to supervisors or regulatory bodies?

From Q1 2018, SWIFT reserves the right to report to supervisors users in their country that have failed to submit a self-attestation.

From January 2019 onwards SWIFT reserves the right to notify local supervisors of users that have failed to confirm full compliance with the mandatory controls or those that connect through a non-compliant service provider.

What information will SWIFT provide when reporting to supervisors?

Reporting is limited to the name of the users and 8-character BIC(s) concerned. Any additional information will need to be obtained on a bilateral basis between the supervisor and the user concerned.

How will SWIFT follow up on non-supervised SWIFT users?

All users with access to KYC-SA can already do a search to see if one of their counterparties has not attested. In Q3, SWIFT will offer the ability to generate a report of your non-attested messaging counterparties. This will only include their attestation status, not content.

We have not submitted our attestation - how does SWIFT know which supervisor to report to?

Users registered with SWIFT as supervised entities will be reported to the primary banking supervisor in their country.

4. 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 are able to store their attestation data and share with other selected users. The KYC registry provides an efficient mechanism to share information with selected counterparties.

How do users consult their counterparties' attestation data?

Users can search the Security Attestation Application for attestations published by other users and request access to view their attestation. This allows you to assess your counterparty attestations in accordance with your cyber risk management framework and policies, alongside other risk considerations such as KYC, sanctions and AML. Using the KYC-SA, you can grant your counterparties access to your self-attestation and request access to the self-attestation of other users. You control access to your attestation – you can grant or deny requests to view your attestation.

How can I be sure that my counterparty's attestation is credible?

Each user is responsible for the correctness and completeness of its own attestation. This is key to support proper counterparty risk management and business decision making processes. If you have any questions on your counterparty's attestation, we encourage dialogue and follow-up with them to discuss any concerns you may have.

What should I do if my counterparty has not attested at all?

All SWIFT users must self-attest. If you have any questions on your counterparty's attestation status, you should check via the KYC-SA, and if necessary initiate a dialogue with your counterparty to discuss any concerns you may have.

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. Each user is automatically subscribed to The KYC Registry Attestation Application. You do not have to be a subscriber to SWIFT KYC Registry services to use this application to self-attest.

What self-attestation information must be provided or validated?

In the KYC Registry Security Attestation Application, the user must provide or, if already pre-completed by SWIFT, validate a standardised set of 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 KYC Registry Security Attestation Application (KYC-SA)?

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

Will SWIFT inform users when the attestation data in the KYC-SA for their counterparties is updated?

The KYC-SA includes an alerting mechanism. Users that have been granted access to view counterparty's attestation data will be informed of subsequent changes to that attestation.

What further enhancements are planned to the KYC-SA?

V3 of the KYC-SA, tentatively planned for the end of Q2 2018, will include general enhancements to improve user experience and ease operations including additional reporting, the ability to identify your messaging counterparts, and better access request management.

Do users have to pay to use the KYC-SA in order to submit security attestation information?

No. The KYC-SA is available to users at no additional charge.

Which languages does the KYC-SA support?

The KYC-SA is available in English. It should also be noted that, if attesting users include additional comments in their attestation, these must be in English

- end -