ODYSSEY™
cybersecurity

SERVICE DESCRIPTION DOCUMENT

SWIFT Auditing Services

Discover

SWIFT CSP Assessment Provider

What is the SWIFT Customer Security Program?

The digital threats faced by the financial sector have never been greater. Since 2016, there has been a continued expansion of the information-threat landscape, with SWIFT users receiving attacks of increasing levels of sophistication. The Tactics, Techniques and Procedures (TTPs) have changed as institutions strengthened security measures. The persistence of such threats underlines the importance of remaining vigilant and proactive in the long-term. While SWIFT users are responsible for protecting their own environments when accessing the SWIFT network, the Customer Security Programme (CSP) was introduced to support them by driving industry-wide collaboration in the fight against cyber fraud. The CSP establishes a common set of security controls known as the Customer Security Controls Framework (CSCF), which is designed to help users secure their local environments and foster a more secure financial ecosystem.

SWIFT's Customer Security Controls Framework (CSCF)

The SWIFT Customer Security Controls Framework (CSCF) consists of both mandatory and advisory security controls for SWIFT users. Mandatory security controls establish a security baseline for the entire SWIFT community, and must be implemented by all users on their local SWIFT infrastructure. These mandatory controls were prioritized to set a realistic goal for near-term, tangible security gain and risk reduction. Moreover, optional advisory controls are based on good practice that SWIFT only recommends users to implement. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

The CSP is designed to be a collaborative effort between SWIFT and its users to strengthen the overall security of the financial ecosystem. All users must therefore read the controls set out in this document carefully, and prepare their own organization accordingly for effective implementation.

How does it help you?

The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can have global implications.

Companies do not operate in a vacuum, therefore, all SWIFT users are part of a broader ecosystem. Even with strong security measures in place, attackers are growing more and more sophisticated, and you must assume that you are already the target of targeted cyberattack campaigns. This is why it is also vital to manage security risk in your interactions and relationships with counterparties.

SWIFT has requested users to set up these cybersecurity controls by 31 December 2017, and to update their systems according to CSP requests on an annual basis. The CSP compliance will come through self-attestation. SWIFT has already announced updates to the Customer Security Controls Framework for attestation in 2021.

SWIFT encourages its users to implement and monitor these customer security controls as part of a broader cybersecurity risk management program, which should be regularly evaluated and adjusted based on leading industry practices as well as changes to the individual users' security posture and infrastructure.

Securing your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber-related fraud.

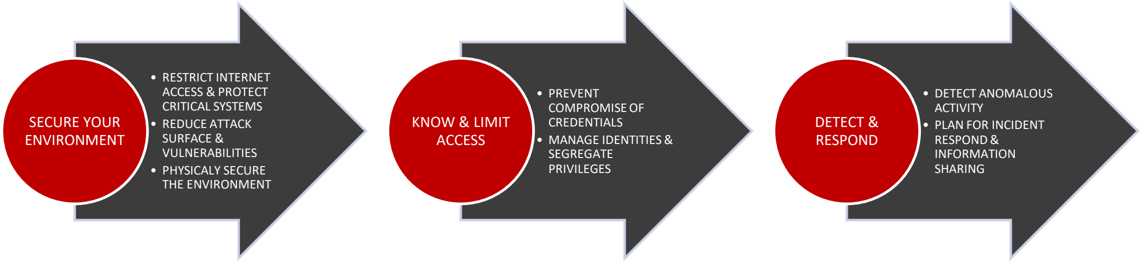
SWIFT CSP controls scope

The scope of the related security controls encompasses a defined set of components in the user's local environment.

In supporting the adoption of the controls, SWIFT has developed a process that requires users to attest compliance against the mandatory and the optional advisory security controls. Users are asked to submit an attestation into the KYC Security Attestation application (KYC-SA). By the end of each year, users must attest compliance with the mandatory and optional advisory security controls as documented in the CSCF in effect at that time. A new version of the CSCF is typically published in early July, listing the mandatory and advisory controls users need to attest against as from July of the following year when implemented in the KYC-SA. To illustrate, users must attest between July and December 2021 against the security controls listed in the CSCF v2021 published mid-2020.

SWIFT's Objectives and Strategic Security Principles

The SWIFT Customer Security Controls Framework is made out of three objectives and seven strategic security principles. The framework is applicable to four types of SWIFT user architectures, titled A1, A2, A3, and B. SWIFT users must first identify which architecture applies to them before implementing the applicable controls.


SECURE YOUR ENVIRONMENT
RESTRICT INTERNET ACCESS & PROTECT CRITICAL SYSTEMS
REDUCE ATTACK SURFACE & VULNERABILITIES
PHYSICALY SECURE THE ENVIRONMENT
KNOW & LIMIT ACCESS
PREVENT COMPROMISE OF CREDENTIALS
MANAGE IDENTITIES & SEGREGATE PRIVILEGES
DETECT & RESPOND
DETECT ANOMALOUS ACTIVITY
PLAN FOR INCIDENT RESPOND & INFORMATION SHARING

SWIFT Architecture Types

Architecture A1 – Users owning the communication interface (and generally the messaging interface)
The communication interface is owned by the user. Users that do not own a messaging interface but own a communication interface only are also considered as architecture A1. The architecture A1 architecture type also includes hosted solutions where the user owns the license for the communication interface that a) they operate on behalf of other user(s), or b) is operated on their behalf by a third party within or (hosted) outside the user's environment.

Architecture A2 – Users owning the messaging interface but not the communication interface. The messaging interface is owned, but a service provider (for example, a service bureau, SWIFT or a group hub) owns the license for the communication interface. This architecture type also includes hosted solutions where the user has the license for the messaging interface that is operated for himself by a third party or a service provider.

Architecture A3 – A SWIFT connector is used within the user environment to facilitate application-to-application communication with an interface at a service provider (for example, a service bureau, a group hub) or with SWIFT services (such as Alliance Cloud, Alliance Lite 2, and in the future, a messaging service or the Transaction Platform exposed by SWIFT).
Optionally, this setup can be used in combination with a GUI solution (user-to-application). In such case, controls pertaining to the GUI also have to be implemented. This architecture type also includes hosted solutions of the SWIFT connector.

Architecture A4 – A server running software application (for example, a file transfer solution or middleware system that are customer connectors) is used within the user environment to facilitate application-to-application communication with an interface at a service provider (for example, a service bureau, a Lite2 Business Application provider or a group hub).
This specific architecture will require some users to adopt the Architecture A4:
- Users that previously attested as B Architectures when using, as customer connector, a middleware server.
- Users that previously attested as A3 Architecture when using, as connector, a file transfer solution or a middleware server.
Those users will have to consider the controls having middleware server in-scope.

To pave the way for the future, this type A4 architecture also includes customer connectors being own applications used within the user's environment that implement SWIFT API's to directly connect and transmit independently business transactions to SWIFT services (a future messaging service or the Transaction Platform exposed by SWIFT). The own implementation of the SWIFT API's (using either the specifications or integrating the SWIFT SDK makes such applications a custom-made API endpoint, referred to as a customer connector or non-SWIFT footprint). This last setup can also integrate a GUI solution (user-to-application). In such a case, controls relevant to the GUI must be implemented as well.

Architecture B – No local user footprint. No SWIFT-specific infrastructure component is used within the user environment. Two types of setups are covered by this architecture type:

– Users only access SWIFT messaging services via a GUI application at the service provider (user-to-application). The PC or device used by those users to submit or affect business transactions must be considered as a general-purpose operator PC, and protected accordingly.

– Users' back office applications communicate directly with the service provider (application-to-application) using APIs from the service provider or a Middleware client, without connecting or independently transmitting business transactions to SWIFT Alliance Cloud, a SWIFT messaging service, the SWIFT API Gateway or, in the future, the Transaction Platform exposed by SWIFT. In such a case, the service provider has to ensure the security of their environment and that of the data exchange, with the user in line with the CSCF controls. Categorizing this setup as architecture type B is in line with the scope of the security controls, which excludes user back-office applications. However, SWIFT strongly recommends already implementing the type A4 architecture controls on these applications, integrating API or a Middleware client.
This architecture type also includes users who only access with a browser, SWIFT messaging services (user-to-application) exposed by Alliance Cloud and Alliance Lite2. PCs used by those users to submit or affect business transactions must be considered as (general purpose) operator PCs and protected accordingly.

The 2021 SWIFT CSP update and its impact

Moreover, from mid-2021, all users will be obligated to perform "Community Standard Assessments". This means that all attestations submitted in 2021 under the CSCF v2021 also require an independent assessment. A user can do this in either of two ways:

1. **External assessment** by an independent external organization, which has existing cybersecurity assessment experience, and individual assessors who have relevant security industry certification(s), or
2. **Internal assessment** by a user's second or third line of defense function (such as compliance, risk management or internal audit) or its functional equivalent [as appropriate], which is independent from the first line of defense function that submitted the attestation (such as the CISO office) or its functional equivalent [as appropriate]. As per external assessors, those undertaking the assessment work should possess recent and relevant experience in the assessment of cyber-related security controls.

Last, separate and distinct from the above two categories, SWIFT also reserves the right to seek independent external assurance to verify the veracity of their self-attestation, as outlined in the Customer Security Controls Policy (CSCP). These are called "SWIFT-Mandated assessments".

SWIFT-Mandated assessments must cover all SWIFT mandatory controls applicable to the user's architecture type as defined in the version of the CSCF applicable at the time the assessment is conducted, even if the assessment request relates to an attestation submitted under a prior version of the CSCF.

HEADQUARTERS

1 Lefkos Anastasiades Str.
2012 Strovolos, Nicosia, Cyprus

T +357 22463600
F +357 22463563
E info@odysseycs.com

www.odysseycs.com

ODYSSEY™
cybersecurity

OFFICES CYPRUS | GREECE | USA | UK | KSA