schellman
Quality. above all.

A Guide to **SWIFT** Cybersecurity Assessments

Is your organization ready for an independent assessment?

SWIFT Customer Security Controls Framework

WHITEPAPER

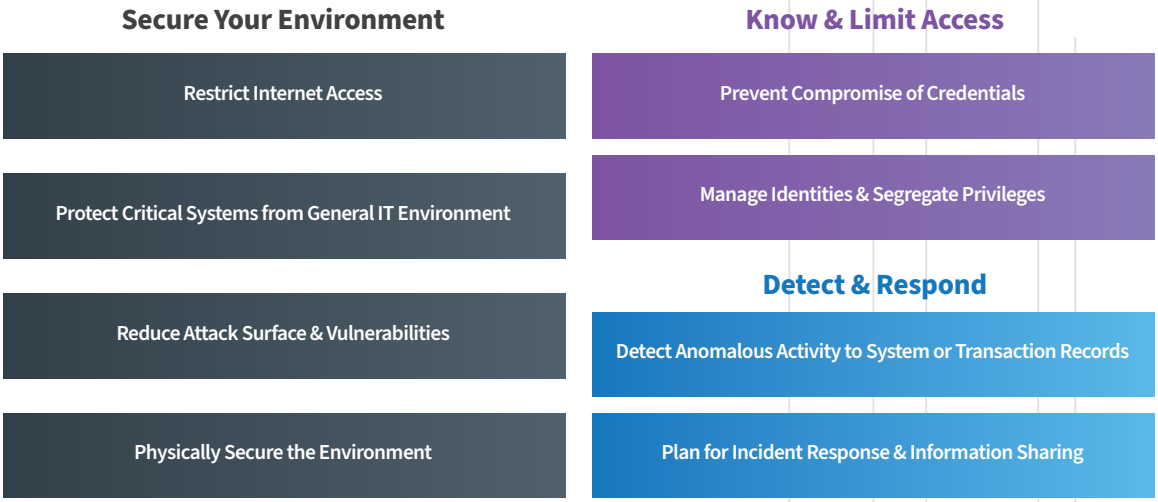
schellman
Quality. above all.

FAQs

What is the SWIFT Customer Security Programme and the Customer Security Controls Framework?

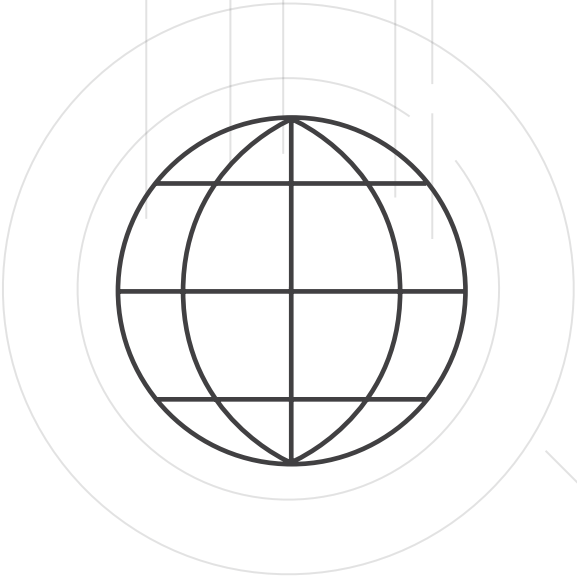
Following several high profile cybersecurity incidents at member organizations in 2016, SWIFT launched its Customer Security Programme (CSP) and issued the Customer Security Controls Framework (CSCF) to establish a baseline of security controls for users to defend against, detect, and recover from cybercrime. The CSCF is updated annually to address new threats and strengthen security controls. Below is a depiction of the framework's objectives and principles.

Framework Objectives & Principles



What's New in the CSCF?

A new version of the CSCF is typically published each year in July. The updates made to the mandatory and advisory controls become effective in the following calendar year. The 2020 version of the CSCF promotes two advisory controls from the previous release to mandatory security controls (Virtualisation Platform Protection and Application Hardening) and introduces two new advisory controls (Restriction of Internet Access and Relationship Management Application (RMA) Business Controls). In addition, the CSCF v2020 extended the scope of certain controls, such as 2.4A Back Office Data Flow Security, to include local infrastructure such as messaging and queuing middleware.
When extending the scope, the new in-scope components can be tagged as Advisory during the initial year.



The CSCF v2021 does not introduce many changes when compared to CSCF v2020. One control is promoted to mandatory and no additional controls have been added. In addition, a number of guidelines and scope definitions have been clarified to better support attestations and assessments. Finally, a new architecture type, identified as A4, has been introduced.

The following page provided by SWIFT shows the change summary of the CSCF since its inception in 2017.

schellman
Quality. above all.

CSP | CSCF Controls Evolution

2017

- 27 Controls
- 16 Mandatory + 11 Advisory
- Self-Attestation by December 31, 2017

2018

- 27 Controls
- 16 Mandatory + 11 Advisory
- Compliance by December 31, 2018

2019

- 29 Controls
- 19 Mandatory + 10 Advisory
- Compliance by December 31, 2019

x3 Promoted to Mandatory
- 2.6 Operator Session Flows
- 2.7 Vulnerability Scanning
- 5.4 Password Storage

x2 New Advisory
- 1.3A Virtualisation Platform
- 2.10 Application Hardening

2020

- 31 Controls
- 21 Mandatory + 10 Advisory
- Compliance by December 31, 2020

x2 Promoted to Mandatory
- 1.3 Virtualisation Platform
- 2.10 Application Hardening

x2 New Advisory
- 1.4A Restrict Internet Access
- 2.11A RMA Controls

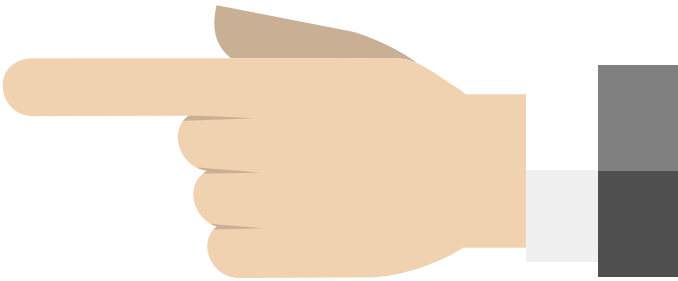
x1 Scope Extension
- 2.4A Back-Office Data Flow - MQ / Middleware Server

2021

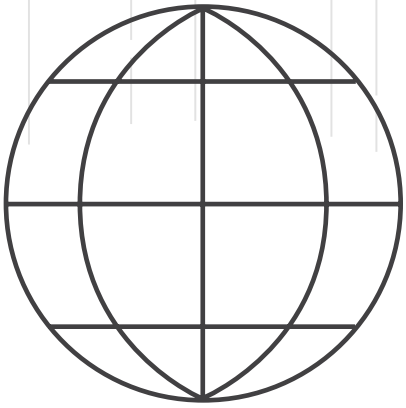
- 31 controls
- 22 mandatory + 9 advisory
- Compliance by December 31, 2021

x1 Promoted to Mandatory
- 1.4 - Restrict Internet Access

x1 - New architecture type added
- A4 for non-SWIFT footprints



WHITEPAPER

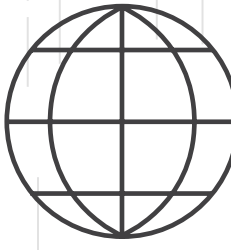


The most significant changes made to the CSCF is the implementation of the Independent Assessment Framework. This framework mandates SWIFT users to perform an independent Community-Standard Assessment.

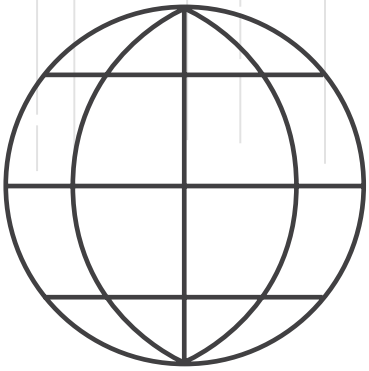
What is the Independent Assessment Framework (IAF)?

Given the mandate for SWIFT users to perform an independent assessment, the IAF provides SWIFT users and assessors with a comprehensive overview of the independent assessment process.

Additionally, the IAF has established assessment templates and forms to provide a consistent approach to the independent assessment process. The templates can be leveraged by assessors to thoroughly capture the details and results of the assessment. Separate templates are available for both the mandatory and advisory control sets. Use of these templates is recommended for both SWIFT Mandated and Community-Standard Assessments.

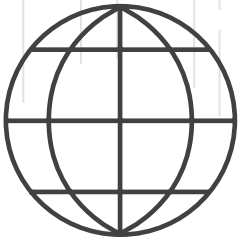


schellman
Quality. above all.



What is a Community-Standard Assessment?

Since 2017, SWIFT users have been required to self-attest to meeting all mandatory security controls in the CSCF. With the recent CSCF updates, users are now required to complete an independent Community-Standard Assessment to support their attestation submission. At a minimum, this assessment must cover all mandatory controls in the latest version of the CSCF that are applicable based on a user's SWIFT architecture type and infrastructure. Furthermore, all Community-Standard Assessments are mandated to use an independent assessor.

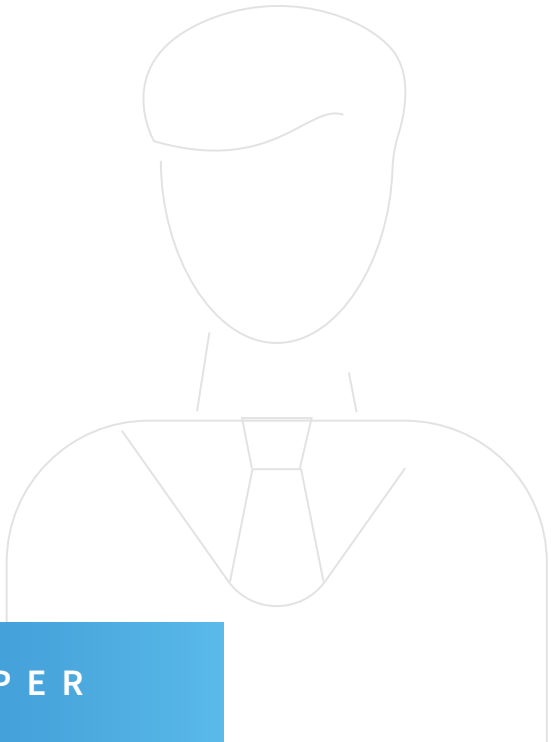


What is meant by “independent assessor”?

To properly execute a CSCF assessment, the assessor must be free from any conflict of interest and demonstrate a level of independence such that the activity is conducted in a reliable and objective manner. SWIFT characterizes ‘independence’ as follows:

Independence is the freedom from conditions that threaten the ability of the audit activity to carry out assessment responsibilities in an unbiased manner. Threats to independence must be managed at the individual auditor, engagement, functional, and organisational levels.

An independent assessor is required for all Community-Standard Assessments. The IAF defines an independent assessor as one “free from any conflict of interest and demonstrate a level of independence such that the activity is conducted in a reliable objective manner.



What are the required qualifications for an external assessor?

The IAF requires that the external assessor have recent (within twelve months) and relevant experience to execute a cybersecurity-oriented operational assessment to an industry standard such as:

- PCI DSS
- ISO 27001
- NIST Cybersecurity Framework
- NIST Special Publication 800-53

Additionally, all individuals tasked with carrying out the assessment should hold at least one industry-relevant professional certification such as:

- PCI Qualified Security Assessor (QSA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- ISO 27001 Lead Auditor
- System Administration, Networking, and Security Institute (SANS)

What is the scope of the Community-Standard Assessment?

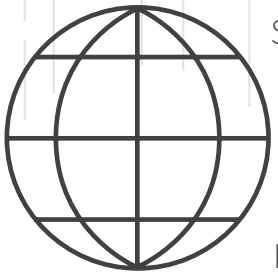
Defining the assessment scope is key to ensuring your assessment meets SWIFT's Community-Standard Assessment requirements. All assessment types must cover all mandatory security controls in the recent CSCF updates that are applicable to the user based on the architecture type and infrastructure. The assessment should confirm the architecture type selected and encompass all production, disaster recovery (DR), and/or backup environments (as applicable) that house any of these systems, operators, or devices. The following non-exclusive list of systems and components are examples of SWIFT-related infrastructure:

- **Data Exchange Layer**
  - Middleware Server is advised for consideration although it is not compulsory

- **Local SWIFT Infrastructure**
  - Secure Zone
  - Messaging Interface
  - Communication Interface
  - SWIFTNet Link (SNL)
  - Connector
  - SWIFT Hardware Security Modules (HSMs)
  - Firewalls, routers, and switches within or surrounding the SWIFT infrastructure
  - Graphical User Interface (GUI)
  - Jump Server
  - Virtualisation Platform
  - Dedicated Operator PC

What is the scope of the Community-Standard Assessment? (Cont.)

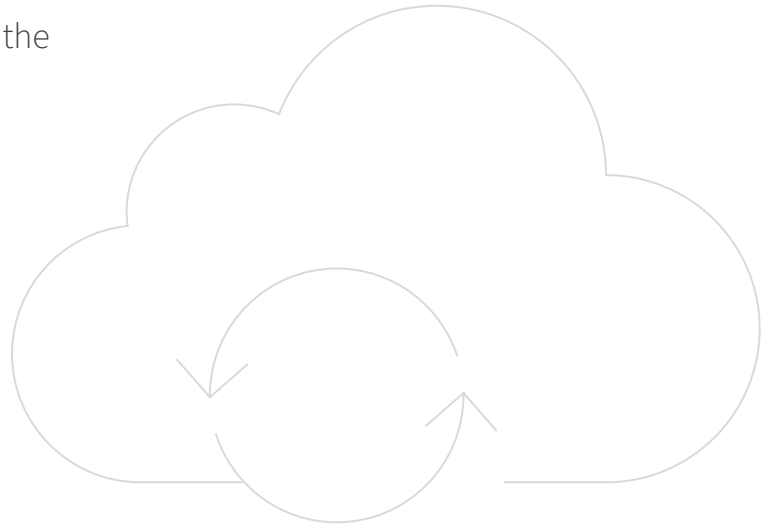
- **Operators and their General Operator PCs**



SWIFT users must self-attest for all in-scope components. This is not limited to just the production / live environment but must extend to back-up and disaster recovery environments as well.

Furthermore, test systems must be fully segregated from the production environment and are required to have the same security measures as the production systems.

Due care should also be exercised to ensure test environments are configured to only support test traffic and data, excluding live production data.



What's my SWIFT architecture type?

Each user must identify which of the four reference architecture types most closely resembles their own architecture deployment to determine which controls are in scope.

The four reference architectures are as follows:

Architecture A1 - Users with communication interface

The communication interface is owned and within the user environment. This architecture type also includes hosted solutions where the user owns (has the license for) the communication interface that he operates or that is operated for himself or on behalf of other user(s).

Architecture A2 - Partial stack without communication interface

The messaging interface is within the user environment, but a service provider (for example, a service bureau, SWIFT Alliance Remote Gateway or a group hub) owns the license for the communication interface. This architecture type also includes hosted solutions of the messaging interface where the user has the license for the messaging interface.

Architecture A3 - SWIFT Connector

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).

Architecture A4 - Customer Connector

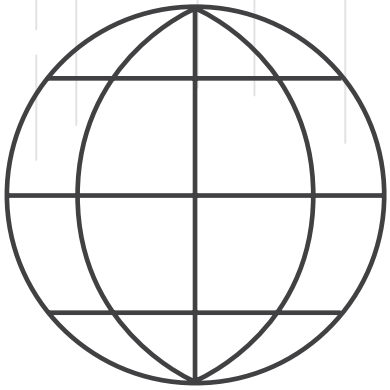
A server running software application (for example, a file transfer solution or middleware system such as IBM MQ server or similar that are customer connectors is used within the environment to facilitate to application-to-application communication with an interface at a service provider (for example, a service bureau, a Lite2 Business Application provider or a group hub).

What's my SWIFT architecture type? (Cont.)

Architecture B – No local user footprint

No SWIFT-specific infrastructure component is used within the user environment. Two types of set-ups are covered by this architecture type:

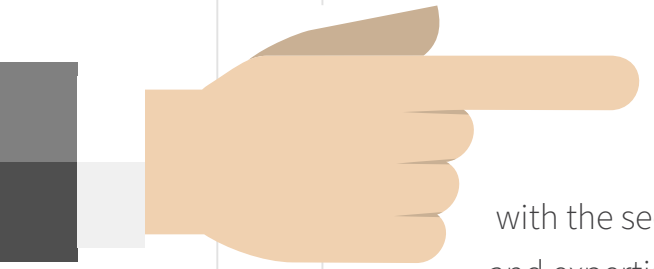
- Users only access SWIFT messaging services via a GUI application at the service provider (user-to-application). The PC or device used by those users should be considered as a (general purpose) Operator PC and protected accordingly.



- Users' back-office applications communicate directly with the service provider (application-to-application) using a middleware product (for example, IBM® MQ or similar) or APIs from the service provider categorizing this set-up as architecture.

- Type B is in line with the scope of the security controls, which excludes user back office and middleware applications. However, SWIFT strongly recommends implementing the architecture type A4 controls on these middleware and API applications.

What is the benefit of utilizing an external assessor?



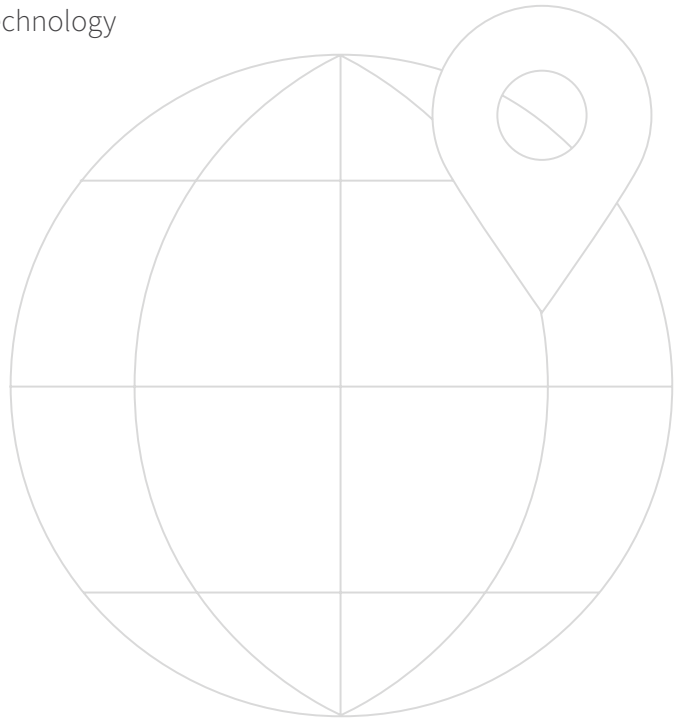
An external assessor can bring valuable insight into the cybersecurity program of a SWIFT user and ensure the proper determination of compliance with the security controls. Moreover, an assessor's experience and expertise with related compliance initiatives will allow you to integrate your SWIFT cyber controls into your overall security program, maximizing value to the overall health of your program.

SWIFT reserves the right to require their users to undergo a mandated external assessment to confirm a user's self-attestation outlined in the Customer Security Controls Policy (CSCP). Establishing an external assessor review cadence would allow SWIFT users to minimize internal resource constraints and afford the user the opportunity to provide the external assessment completion letter to SWIFT if the user was chosen for a mandated assessment.

How can a SWIFT independent assessment strengthen my compliance and security programs?

SWIFT's development of the CSCF was a collaboration of internal and external industry experts. Due care was taken to ensure the framework was closely aligned with other reputable industry compliance standards. As such, the practice of these controls are not only valuable in the SWIFT environment, but also to the security of the organization's overall program. The CSCF includes a mapping to three international security standard frameworks:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1
- ISO 27002 (2013)
- Payment Card Industry Data Security Standard (PCI DSS) v3.2.1



How can Schellman help?

To prepare for the SWIFT assessment, Schellman can conduct gap analyses to determine if current controls satisfy the SWIFT CSP requirements. When you're ready to validate successful compliance with the SWIFT CSP controls, Schellman can perform the attestation and assurance activities for SWIFT compliance. Schellman is also perfectly positioned to include additional regulatory standards as part of a holistic cybersecurity audit. Additionally, Schellman can:

- Evaluate the maturity level of cybersecurity programs and provide critical feedback to senior leadership.
- Provide additional oversight as a third party.
- Schellman's team of security assessors includes leading experts in various information security regulatory standards, such as SOC, PCI, ISO, FedRAMP, and HITRUST.
- Add peace of mind to your organization's assessment by allowing Schellman to validate that mandatory controls are being implemented as required.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.813.288.8833