

# SWIFT

## Reinforcing the Security of the Global Banking System

As of July 2021, the SWIFT Customer Security Controls Framework (CSCF) will require an independent assessment under the guidance provided in the SWIFT Independent Assessment Framework (IAF). Let's highlight and answer some of the more commonly asked question regarding compliance with the SWIFT CSCF under the IAF and discuss a few of the more challenging controls to implement.



# What is SWIFT?

The Society for Worldwide Interbank Telecommunications (SWIFT) is a global cooperative of financial and technology organizations which enables a standardized, reliable, and secure transmission of transaction messages. This includes provision of SWIFT-branded software components that communicate with the SWIFT network. In short, SWIFT facilitates financial transactions among participating member organizations across the globe.



# What controls must be implemented to be compliant with SWIFT CSP?

All users of the SWIFT network are required to attest to their compliance with the mandatory controls specified in the CSCF. This security-focused framework contains three objectives which are: Secure Your Environment; Know and Limit Access; and Detect and Respond. Mandatory and advisory control statements and security principles are organized beneath these three objectives and are applicable based upon your organization's SWIFT architecture.

## Framework Objectives & Principles

### Secure Your Environment

Restrict Internet Access

Protect Critical Systems from General IT Environment

Reduce Attack Surface & Vulnerabilities

Physically Secure the Environment

### Know & Limit Access

Prevent Compromise of Credentials

Manage Identities & Segregate Privileges

### Detect & Respond

Detect Anomalous Activity to System or Transaction Records

Plan for Incident Response & Information Sharing

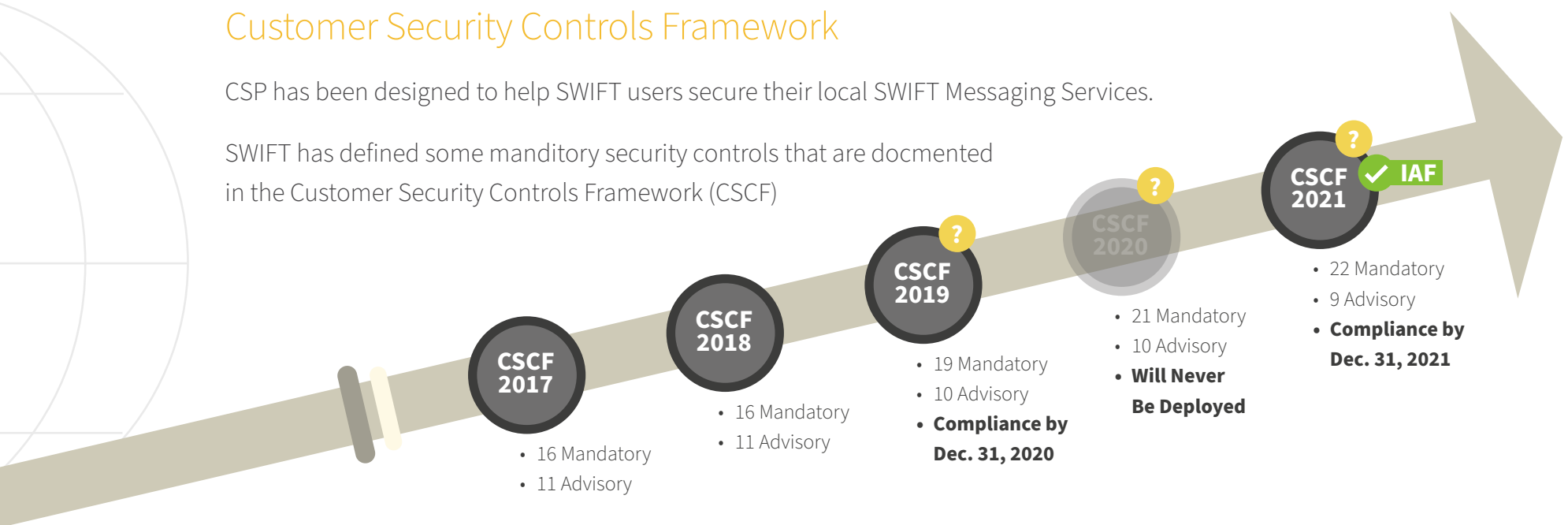
# What is changing with the 2021 version of the CSCF?

If your organization has not yet completed an independent assessment of compliance with the CSCF, 2021 is the year to pursue this obligation. Due to the constraints upon organizations resulting from the COVID-19 pandemic, SWIFT extended the version lifecycle of the CSCF by promoting only one control from advisory to mandatory. While certain remaining advisory controls are expected to eventually become mandatory, the transition from v2020 to v2021 leaves the compliance burden somewhat unchanged.

## Customer Security Controls Framework

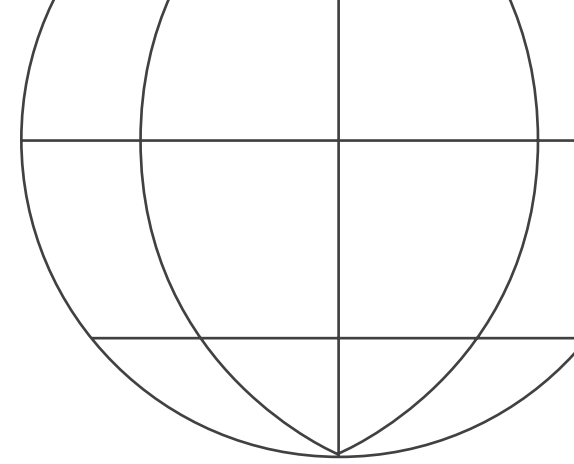
CSP has been designed to help SWIFT users secure their local SWIFT Messaging Services.

SWIFT has defined some mandatory security controls that are documented in the Customer Security Controls Framework (CSCF)



# Promoted Control:

## 1.4 Restriction of Internet Access



The only control promoted from advisory to mandatory for the 2021 version of the CSCF, restricting internet access, is also one of the more challenging controls for clients to successfully implement. Breaking down this control into its primary implementation guidelines is helpful when seeking to understand the actions your organization may need to consider in order to successfully comply with this particular control. First, we need to consider the secure zone and limit our connectivity there. While the implementation guidelines indicate that servers can communicate outbound to the internet with the use of whitelisted URLs or a proxy, dedicated operator PCs and jump servers inside the secure zone must be prohibited from internet access. Jump servers are mentioned as a key component in the implementation guidance and should certainly be considered as a way to comply. Another more restrictive approach here is to conduct all activity that requires internet access outside of the secure zone where possible. Secondly, we must examine our middleware systems in use, including hypervisors and messaging servers. Again, the implementation guidelines give us some flexibility here to use URL whitelisting with content inspection. Once we break down this control to its essential requirements, a compliant implementation seems far easier.



An illustration of a stylized globe with green continents and blue oceans. Several icons are placed around the globe: a classical building with a dollar sign on its roof, a padlock, and a classical building with a dollar sign on its roof. Dashed white lines connect these icons across the globe. In the top left corner, there are grey clouds.

# CSCF Controls Topics


Another challenging area for compliance surrounds CSCF control 7.1 Cyber Incident Response Planning. While the guidance for this control certainly incorporates many well-known industry standards and best practices, the nuanced considerations necessary for SWIFT users to implement often introduces a curve ball to many organizations. Let's take for example the requirement for SWIFT users to incorporate the Cyber Security Incident Recovery – roadmap as detailed in SWIFT-ISAC Bulletin #10047 into the overall incident response plan. This is often an overlooked detail that is a critical component of a SWIFT user's incident response plan. A second implementation guidance detail often excluded from incident response plans is specific to the organization's capability to consume and operationalize threat intelligence provided by SWIFT. The SWIFT Indicators of Compromise portal contains useful threat information that should be distributed to responsible security teams within the organization. Ultimately, the details required to comply with the 7.1 can be easily incorporated into the incident response program for a holistic and thorough approach to incident response.




# CSCF Controls Topics (cont.)



Another challenging area for compliance continues to be the application of multifactor authentication (MFA) in a way that complies with the SWIFT CSCF 4.1. Let's break this down into what SWIFT expects for MFA and where we should apply it. First, SWIFT outlines MFA in the industry-accepted and commonly known definition as supplying two factors from something you know (knowledge factor), something you have (possession factor), or something you are (inherent factor). SWIFT's implementation guidance for possession factor includes often-used solutions such as physical USB tokens, smartcards, OTP / TOTP generated on a mobile phone, and RSA tokens. While not an inclusive list, these methods provide a great deal of flexibility for users to comply with this control. As far as logical application of MFA, SWIFT guidelines specifically require for all administrative users to be challenged with MFA in at least one authentication step when accessing a SWIFT system or application, at either the boundary of the secure zone or on the jump server or dedicated operating PC. Similarly for users, MFA must be included in one step of the authentication process prior to accessing the SWIFT application, secure zone, or dedicated operator PC. Following the CSCF implementation guidelines in these regards will ensure an organization is on its way to compliance.

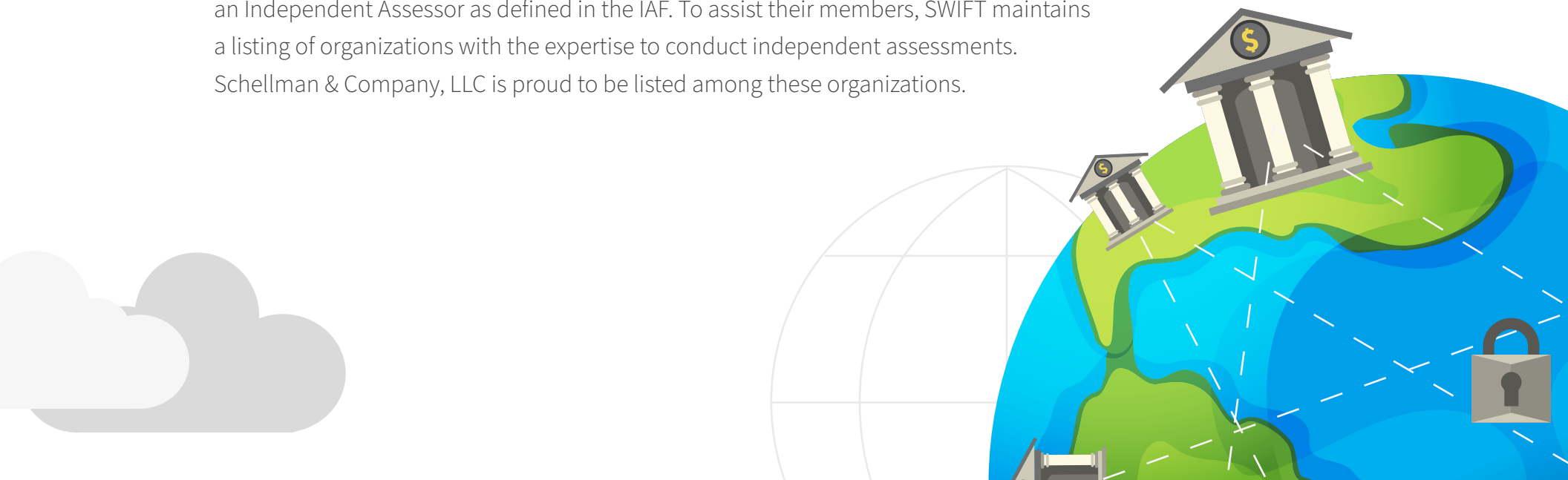


SWIFT's implementation guidance for possession factor includes often-used solutions such as physical USB tokens, smartcards, OTP / TOTP generated on a mobile phone, and RSA tokens.

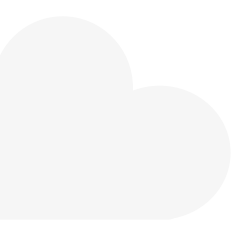


# So how do I attest and what is an independent assessment?

Users of the SWIFT organization are provided with access to the Know Your Customer Security Attestation (KYC-SA) portal, in which they may submit their security attestation which demonstrates their compliance with the CSCF. All users must re-attest annually and before the expiration of the most current version of the CSCF, or before 31 December. In previous versions of the CSCF, it was possible to self-attest compliance through the use of this portal, however; this will change in July of 2021 with the self-attestation model being replaced by the Community Standard Assessment. Starting from July 2020 and going forward, all SWIFT users were obligated to execute these Community Standard Assessments via an Independent Assessor as defined in the IAF. To assist their members, SWIFT maintains a listing of organizations with the expertise to conduct independent assessments. Schellman & Company, LLC is proud to be listed among these organizations.






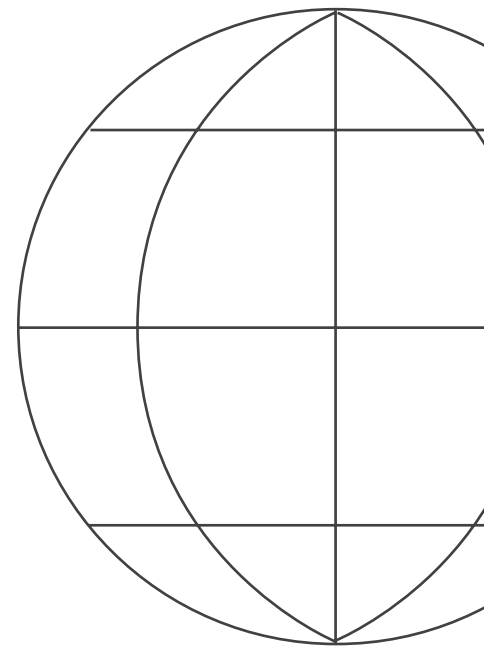


# What can I expect upon completion of an Independent Assessment?

Once Schellman has completed the assessment, your organization will be provided with a disposition describing compliance with each of the applicable mandatory or advisory security controls in the form of a detailed controls summary report. In addition to describing compliance with the CSCF, the controls summary report provides enough detail to assist with your communications regarding organizational cyber security posture to executive leadership. Additionally, your organization will be provided with a letter of compliance to share with your stakeholders to assist with satisfying any contractual or regulatory requirements. Finally, your organization will be provided with a KYC-SA friendly controls summary for completing your attestation in the KYC-SA tool. As a registered SWIFT Cyber Security Service Provider, Schellman has access to SWIFT-specific tools, guidance, and templates, ensuring your assessment is conducted as described by the IAF.



Additionally, your organization will be provided with a letter of compliance to share with your stakeholders to assist with satisfying any contractual or regulatory requirements.



# Wrap It Up

Now is the time to start planning your compliance with the independent attestation requirement under SWIFT's IAF. The framework is based upon industry-accepted and best practices and maps directly to PCI, NIST CSF, and ISO 27001:2013. As a requirement for SWIFT users and an excellent framework for establishing a baseline information security program, Schellman can assist with your planning and compliance efforts.



CLICK FOR MORE INFO

[www.schellman.com](http://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

