How do you lock all the doors technology opens?

SWIFT CSP independent assessment

The better the question. The better the answer.
The better the world works.

Building a better working world

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a member-owned cooperative that establishes international standards for syntax in financial messages, provides a secure network to transmit messages between financial institutions and develops software to connect to the SWIFT network.

Overview

In response to the 2016 Bangladesh SWIFT fraud and resultant publicity, SWIFT has implemented the Customer Security Program (CSP) to address cyber risks for global payments and to enhance trust within the SWIFT community, including financial institutions and other large corporations with connections to the network. Its underlying framework establishes a set of security controls designed to help customers protect against cyber threats and to secure their local infrastructure used to access the SWIFT network. Under the CSP, SWIFT requires that all customers annually self-assess their compliance posture within the Know Your Customer (KYC) tool. KYC is used by SWIFT and customers' counterparties (i.e., other banks, corporations) to view results of the self-attestation.

Currently, SWIFT customers are required to perform self-attestations with little to no involvement from parties independent of the first line of defense (generally treasury) in assessing the information provided to SWIFT. Beginning in July 2021, updates to the CSP will require customers to obtain an independent assessment against SWIFT's framework annually to inform management's self-attestation. This may be accomplished through either:

- **External assessment** by an independent external organization that has existing cybersecurity assessment experience and individual assessors who have relevant security industry certifications. An example of such an external assessment is a CPA's attestation report.
- **Internal assessment** by a user's second or third line of defense function (compliance, internal audit), independent of the first line of defense submitting the attestation. Those that undertake the assessment should possess recent and relevant experience in the assessment of cybersecurity controls.

SWIFT's CSP will require an independent assessment to inform management's self-attestation. As a result, EY has developed an attestation report to meet this need.

Preparing for 2021

Cyber attacks are becoming increasingly sophisticated in the financial community. The SWIFT architecture housed within customer environments facilitates the communication of financial messages (e.g., wire payments) and, due to the increased connections outside of an entity's network, presents additional attack vectors that can be exploited. If not appropriately secured, there is a greater risk of wire fraud, including unauthorized changes to the amount and/or receiver of the funds during final steps of the SWIFT transfer process.

The EY organization is positioned to help meet this need by leveraging a vast network of professionals with broad knowledge and experience in payments, cybersecurity, financial services regulatory compliance and technology risk management to perform a targeted SWIFT CSP attestation, and to prepare a third-party shareable report that communicates your entity's design and implementation of SWIFT's mandatory controls as of the date of the report.

SWIFT CSP attestation report — use and benefits

The attestation report reduces the time and expense needed to address the needs of SWIFT, its customers and other counterparties for trusted risk-based information by allowing organizations to demonstrate that appropriate controls have been designed in their SWIFT environment.

What are the requirements of the SWIFT CSP independent assessment?

At the foundation of the CSP is a controls framework, much like other security frameworks (NIST, ISO, etc.) that exist today. SWIFT's Customer Security Controls Framework (CSCF) is broken into objectives, principles and controls. Controls are further subdivided into a common set of mandatory and advisory security controls, and the number of controls assessed will be dependent on the type of architecture in place at each SWIFT customer.

Architecture A controls	21 mandatory	Objectives	10 advisory
A1: Full stack	10	Secure your environment	6
A2: Partial stack	5	Know and limit access	1
A3: Connector	6	Detect and respond	3
Architecture B controls	**14 mandatory**	**Objectives**	**8 advisory**
B: No local user footprint	5	Secure your environment	5
	5	Know and limit access	1
	4	Detect and respond	2

SWIFT by the numbers

37.9m FIN messages per day[1]

11,000+ institutions connected to SWIFT[2]

200+ countries/territories connected[2]

[1] https://www.swift.com/about-us/swift-fin-traffic-figures
[2] https://www.swift.com/about-us

SWIFT fraud statistics

40% banks that are "very confident" in detecting cyber SWIFT fraud[3]

$380m in SWIFT payment fraud losses since 2016[3]

60% US banks targeted with SWIFT fraud[3]

[3] https://www.eastnets.com/news/eastnets-swift-cyber-fraud-survey-report-reveals-more-than-4-out-5-banks-are-targeted

SWIFT customer security controls framework

3 objectives

- Secure your environment
- Know and limit access
- Detect and respond

8 principles

- Restrict internet access
- Segregate critical systems from general IT environment
- Reduce attack surface and vulnerabilities
- Physically secure the environment
- Prevent compromise of credentials
- Manage identities and segregate privileges
- Detect anomalous activity to system or transaction records
- Plan for incident response and information sharing

31 controls

SWIFT has also defined minimum responsibilities for its customers, as well as the assessors performing the independent reviews:

Assessors' responsibilities — the assessor must provide customers with:

- A formal report describing the assessor's confirmation of compliance for each control, along with documentation of observed implementation defects
- A completion letter confirming the work was done with the required objectivity and independence and with sufficient scrutiny

SWIFT customers' responsibilities — when selecting an assessor, customers must verify and confirm the following:

- The assessor is independent and free from any conflict of interest.
- The firm/internal department conducting the assessment has recent (within 12 months) and relevant experience to execute a cyber-oriented operational assessment to an industry framework or the CSCF.
- Each individual tasked with carrying out the assessment holds at least one industry-relevant professional certification (CISA, CISSP, CISM, etc.).

What challenges are organizations facing?

Many organizations are unable to satisfy the independence and expertise criteria as their second- or third-line functions may have not performed SWIFT assessments in the past or do not have the relevant experience or professional certification.

Some additional challenges we have identified from previous assessments:

- Organizations are not always aware of their business identifier codes (BICs), how many they have, who owns them or who uses them.
- Ownership of the different components of the SWIFT messaging system — business and technology — are not always clearly defined.
- Documentation is insufficient to support the attestation made in the KYC Security Attestation (KYC-SA) tool should SWIFT or a counterparty request further detail on the submission.
- Not all SWIFT infrastructure is appropriately located within the SWIFT "secure zone."
- The SWIFT risk drivers are not always considered in the context of achieving the overall control objective and addressing the implementation guidance.

What are the consequences of noncompliance?

- If the self-attestation submission in the KYC-SA tool is incomplete, this can become visible to counterparties.
- Organizations are using SWIFT KYC-SA counterparty risk information to inform third-party risk management decisions. Noncompliance could have broader impacts on third-party relationships.
- Regulators within the jurisdiction of each SWIFT user can request access to the SWIFT CSP attestation information.
- SWIFT reserves the right to perform on-site, SWIFT-mandated assessments and/or to disconnect a user from the network.
- The CSP framework is designed to focus on key controls for managing cybersecurity risks to the SWIFT system. Noncompliance puts an organization at greater risk of cyber attack.

How EY teams can help

Over 50 SWIFT-certified EY professionals have performed dozens of SWIFT CSP assessments across the globe, working with some of the largest banks, regional banks, wealth and asset management companies, insurance companies, and nonfinancial services clients on enhancing the security and resiliency of the SWIFT messaging system.

Key questions you should ask yourself

- Do I have appropriately qualified and certified personnel to conduct the assessment?
- Is my assessment being performed by an independent function?
- By mid-2021, am I sure that I will comply with all the combined mandatory controls of the SWIFT CSP v2020?
- Have I considered compliance with advisory controls, which may become mandatory in the future?
- Do I know who owns my SWIFT infrastructure, how many BICs my organization has and how they are used?
- Does my organization have a plan to manage SWIFT compliance on an ongoing basis, as the framework evolves?

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 006245-20Gbl
2008-3575115
ED None

ey.com