Building a better working world

SWIFT Customer Security Program

Time to get ready

Key dates

- Start of Q2 2017: First annual self-attestation against 16 mandatory controls
- 1 January 2018: SWIFT starts enforcement, inspections and disclosures on noncompliance against the mandatory controls; customers can expand their disclosures to cover advisory controls

Immediate next steps

- Establish cross-functional team to oversee CSP implementation, including risk, compliance, technology, legal and operations
- Conduct readiness assessment against mandatory and advisory controls
- Assess how attestation requirements align with existing Service Organization Control (SOC) reporting
- Determine how SWIFT CSP effort should align with broader payments cybersecurity initiatives
- Review past audit, risk, IT/information security findings/assessments to identify critical gaps to be addressed as part of CSP implementation
- Evaluate where manual interventions are required for processing to determine potential technological solutions

Over the past few years, financial services policymakers and regulators have realized that it is now a matter of when, not if, the industry will suffer a major system-wide disruption, one that aims to destroy. Well-publicized attacks in the last 12 months have made this feel probable, not just plausible. Not surprisingly, the regulatory focus has increasingly shifted to systemic cyber risks and the weakest links across the system, not just within regulated institutions. New or proposed regulatory standards are being issued more frequently.

Within this shift, there is an even more enhanced focus on the security of the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT Chief Executive Officer Gottfried Leibbrandt said of the attacks on the Bangladesh Bank, "[They] will prove to be a watershed event for the banking industry; there will be a before and an after Bangladesh."[1] Enhancing SWIFT security is critical for global financial markets. After all, it processes 6.5 billion transactions a year, of which a significant minority (around 15%) are processed with manual intervention, and it has more than 11,000 customers.

SWIFT's most prominent new initiative is its Customer Security Program (CSP), which takes effect this year. As of second quarter of 2017, SWIFT's customers now have to attest to complying with 16 mandatory controls (11 for architectures where a third party manages the customer's connection to SWIFT). Any new customers who wish to connect to the SWIFT network must have submitted their self-attestation to SWIFT before they can join. In January 2018, SWIFT may start sharing information on noncompliance with customers' regulators and counterparties, and may, in certain cases, select customers who will need to provide additional assessments performed either from their internal auditors or their external auditors. SWIFT customers will have the option to adopt 11 more advisory (i.e., voluntary) controls and to go beyond self-attestation to self-inspection by internal audit, or third-party inspections.

The CSP covers a range of issues that are now becoming commonplace in new and more demanding — and now increasingly mandatory — requirements, notably the need for:

- Strong access, privilege, password and database controls, and multi-factor authentication

[1] Martin Arnold, "Swift outlines fightback against cyber theft," *Financial Times*, 23 May 2016.

- Detailed knowledge of, and controls over, data flows linkages to business processes
- Effective, timely and robust situational awareness; vulnerability and penetration testing; scenario analysis; detection and anomaly analytics; and incident response
- Integrated people strategy, including training and segregation of duties
- Thorough logging, monitoring and audit processes

Taken together, these new requirements will be demanding on firms and come at a time when other new regulatory requirements are being rolled out. Inevitably, implementing the CSP will precipitate a broader evaluation of each firm's SWIFT security, including potential enhancements to technology, as well as the firm's approach to insider threats, fraud detection and prevention, and cybersecurity controls.

To help, this alert covers:

- Why the CSP is significant
- What the CSP entails
- The key implementation questions to be addressed

Why the CSP is significant

SWIFT is well aware of the potency of cyber attacks. "Cyberattacks are growing in number and sophistication and attackers are focusing more deeply inside banks."[2] It also knows that "combatting fraud is a challenge for the whole industry – there are no quick fixes. The threat landscape adapts and evolves by the day, and both SWIFT and its customers have to remain vigilant and proactive over the long term."[3] Cyber risks now have to be viewed system-wide, not just institution by institution.

SWIFT's CSP is a significant contribution to international payments security. In launching it, Leibbrandt noted, "While customers remain responsible for protecting their own environments, SWIFT is fully committed to helping strengthen customers' security and helping them improve their security measures."[4] SWIFT Chairman Yawar Shah commented, "We recognize this will be a long haul and will require industry-wide effort and investment, as well as active engagement with regulators. The growing cyber threat requires a concerted, community-wide response." [5]

Many in the industry – firms and regulators – agree with this sentiment. However, there is a danger that the industry is not sufficiently focused on implementing the CSP and the other necessary changes that would better secure the SWIFT network, notably technology enhancements. To some degree, that may be because firms sometimes treat SWIFT differently than they do payments systems. First, it's a communication system, so it does not get the same visibility or investment. Second, SWIFT does not have enforcement capabilities that regulators do, so compared with implementing new regulatory requirements, it can be viewed as lower priority. Third, for large firms, SWIFT's CSP mandatory controls may be viewed as relatively baseline security controls, so firms may assume that little action is required.

However, there are a number of reasons to focus more on making SWIFT secure:

- **High volume.** The transaction volume is staggering – 6.5 billion+ messages were sent through the system in 2016, or on average 25 million+ a day.[6] These transactions have a highly predictable format, so they're harder to protect.
- **Manual processing.** More than 15% of transactions still involve manual processing – that's almost one billion transactions a year.[7] Technology upgrades are likely needed to reduce reliance on manual intervention.
- **Limited risk oversight or input.** The SWIFT process is managed, for the most part, by first-line operational professionals. Few firms have sufficient – and in some cases, any – oversight or engagement by the chief information security officers (CISOs) or second-line technology or cyber risk professionals. Internal audit may relegate SWIFT below other payment systems in its plan. However, with the overall trend in cyber risk management toward a three-lines-of-defense approach to addressing cyber risks, all lines will need to consider cyber risks around SWIFT.
- **Subject to the weakest link.** SWIFT has a significant number of customers – more than 11,000 in 200+ countries – so it is very much exposed to the weakest link in the system.
- **Of great interest to key stakeholders.** Regulators and other counterparties will be very focused on the degree to which firms have implemented the SWIFT CSP, and how far firms go in implementing and testing mandatory and advisory controls. Those that go the furthest may gain competitive advantage in the marketplace.
- **SWIFT security needs to be aligned with broader payments security.** Overall, payments fraud has been increasing in recent years, so firms are having to respond with more sophisticated and effective fraud and security

[2] "SWIFT Customer Security Programme FACTSHEET," Society for Worldwide Interbank Financial Telecommunications, September 2016

[3] *Ibid.*

[4] "SWIFT introduces mandatory customer security requirements and an associated assurance framework,"Society for Worldwide Interbank Financial Telecommunications, 29 September 2016.

[5] *Ibid.*

[6] About US," *SWIFT website*, https://www.swift.com/about-us.

[7] "Fund Processing Standardisation: Tracking industry progress – Mid 2016 Update," European Fund and Asset Management Association and Society for Worldwide Interbank Financial Telecommunications.

- controls and new technologies. Enhancements to SWIFT security have to leverage, and be combined with, these broader payments security upgrades.

What the CSP entails

The CSP is based on a multipronged initiative tied to five strategic SWIFT priorities:

1. **Improve information sharing among the global community.** SWIFT wants more information sharing between itself and its customers, including on suspected fraudulent activity, effective preventive and detective measures, and leading practices and innovations on cyber defenses. It will maintain an up-to-date malware inventory and curate an information sharing community.
2. **Enhance SWIFT-related tools for customers.** SWIFT intends to strengthen requirements for consumer-managed software, strengthen its own products, and enhance logging and reporting. This will include enhanced authentication and encryption, user and password management, and integrity checking.
3. **Enhance security guidelines.** SWIFT customers will need to meet certain security and operational baseline standards to manage communications, within new assessment frameworks and certification processes. Baseline standards will include physical and logical access control and segregation of duties.
4. **Support increased transaction pattern detection.** SWIFT will explore new tools to conduct automated transaction pattern detection, to detect anomalies on its system, and to enable customers to recall fraudulent payments messages quickly.
5. **Enhance support for third-party providers.** SWIFT will seek out ways to foster a secure ecosystem of third parties, including providers of relevant and quality security software and hardware, consulting and training, fraud detection solutions, service bureaus, and auditors.

SWIFT launched three enablers to support these strategic priorities:

- Customer and third-party assurance frameworks, which would cover security guidelines and the assurance framework for third parties
- Customer and third-party engagement, which includes a broad-based customer engagement strategy (e.g., through conferences or local events) and direct engagement of CISOs and other subject-matter resources
- Program communications, including through its website, collateral and regional events

At its core, the CSP requires certain mandatory controls and encourage voluntary adoption of other advisory controls, with the objective of getting customers to improve their ability to secure their environment, know and limit access, as well as detect and respond.

SWIFT has defined four architecture types:

- **A1**: full stack
- **A2**: partial stack
- **A3:** connector
- **B**: no local user footprint

A customer is required to identify the type of SWIFT architecture they have, which determines the mandatory and advisory controls the customer must attest to, and the architecture components the controls need to cover. Customers with architecture type "A" (A1, A2 or A3) must attest to 16 mandatory controls and may voluntarily attest to 11 advisory controls, while those with architecture type "B" must attest to 11 mandatory controls and may voluntarily attest to 9 advisory controls. The controls apply to all SWIFT customers and to the whole end-to-end transaction chain, beyond the SWIFT local infrastructure. SWIFT is seeking to implement controls that map well to other industry standards, e.g., those of the National Institute of Standards and Technology.

For each mandatory and advisory control, SWIFT has released so-called control statements, or definitions. After consulting with industry on those statements, SWIFT published final control statements in Q2 2017. The full set of objectives, principles and controls can be found in Table 1 on page 5, with the associated architecture.

The key implementation questions to be addressed

Implementation of SWIFT's CSP begins now. Going forward, customers have to self-attest to the mandatory controls.

As firms develop their implementation strategy, they have six key questions to address:

1. **Should advisory controls be adopted?** Customers have no choice but to implement the 16 mandatory controls (11 for architectures where a third party manages the customer's connection to SWIFT), but they do have to determine whether to voluntarily adopt some or all of the 11 advisory controls (9 for architectures where a third party manages the customer's connection to SWIFT). As shown in Table 1, this means focusing more attention and investment on controls associated with reducing attack surface and vulnerabilities, managing identities and segregate privileges, detecting anomalous activity to systems or transaction records, and planning for incident response and information sharing.
2. **Should we go beyond self-attestation on compliance?** Starting in the second quarter of 2017 — and annually thereafter — customers will have to self-attest to compliance against the mandatory controls. Additionally, SWIFT customers can decide to conduct more stringent inspections to show compliance — including against the advisory controls. The customer user must choose the type of assessment the self-attestation is based upon, which can be a combination of a self-assessment, an internal audit and / or an external audit. In the case of an external audit, the name of the assurance provider must also be specified. Firms will need to develop their own attestation program, including coverage of each specific control and how these assessments will be undertaken and documented.
3. **What information should be disclosed?** SWIFT will begin disclosing information to counterparties about customers' compliance with the mandatory controls in January 2018. They will also start selecting customers to provide additional assurance from their internal and external auditors on their self-attestation, and reserve the right to disable a customer's connection to the network. In this context, firms will have to determine what disclosures they will make about their compliance and approach to the CSP, including their decision on advisory controls and their approach to evaluating compliance.
4. **How should we engage the CISO, risk professionals and others across the firm?** To be successful, firms should engage CISOs and second-line technology and/or cyber risk professionals in their CSP implementation strategy. This will help confirm the program is getting the right level of visibility and investment across the firm and is properly linked to the broader cyber risk management strategy. More broadly, other groups need to be engaged, including business unit executives, technology delivery and management, operations, legal, compliance, and operational risk.
5. **How should SWIFT compliance be linked to other cyber regulatory and risk programs?** Firms will need to determine how their CSP implementation program maps to other major cyber initiatives, especially those related to new or proposed regulation. While many new requirements have their own specific focus, it is important that firms take an integrated approach, such that they leverage enhancements being made for one reason in other areas — the aim should be to address multiple regulatory or industry requirements with one integrated change and risk management program. A siloed approach that treats all new requirements separately may be costly, inefficient and ultimately less effective in properly enhancing the firm's approach to cybersecurity.
6. **What technological enhancements are required?** In many cases, when firms undertake a robust assessment against the mandatory and advisory controls, they may identify some material technological enhancements that should be implemented. Some will relate directly to the CSP — for example, deploying pattern behavior monitoring across the SWIFT ecosystem, enabling regular red-teaming exercises to test cyber resiliency of payment controls in light of changing threat actors, and deploying local intrusion detection technology on all critical SWIFT systems. However, broader technological priorities will likely surface, notably those related to greatly reducing dependency on manual processing — after all, automation significantly reduces opportunities for fraud and error rates.

With so much attention on new cyber risk management regulatory proposals regulators, it would be easy to relegate SWIFT's CSP down the priority list. However, that would be a mistake. SWIFT's CSP is demanding, and almost upon the industry. Acting now is critical.

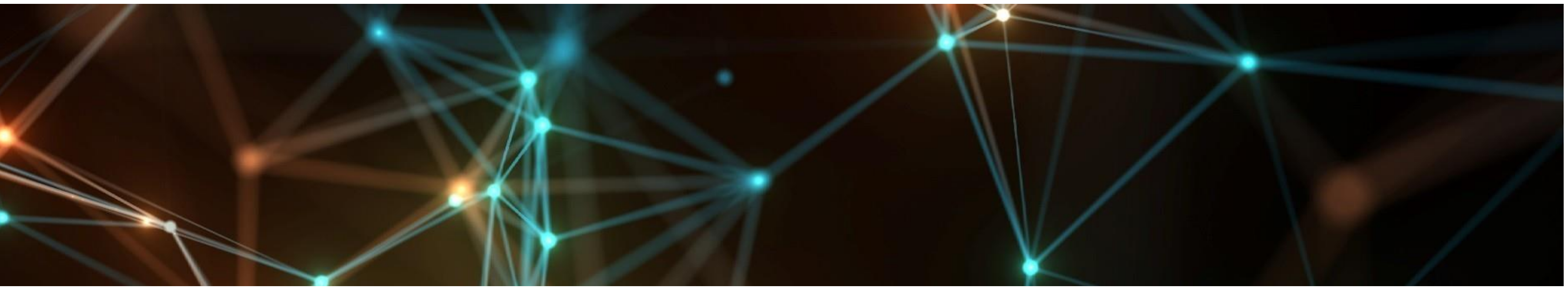

Table 1: SWIFT CSP control requirements[8]

Objectives	Principles	Controls	Architecture A	Architecture B
Secure your environment	Restrict internet access and segregate critical systems from general IT environment	Mandatory controls		
		SWIFT environment segregation: ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment	✓	
		Operating system privileged account control: restrict and control the allocation and usage of administrator-level operating system accounts	✓	
	Reduce attack surface and vulnerabilities	Mandatory controls		
		Internal data flow security: ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC	✓	
		Security updates: minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk	✓	✓
		System hardening: reduce the cyber attack surface of SWIFT-related components by performing system hardening	✓	✓
		Advisory controls		
		Back-office data flow security: ensure the confidentiality, integrity and mutual authenticity of data flows between back-office (or middleware) applications and connecting SWIFT infrastructure components	✓	✓
		External transmission data protection: protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone	✓	
		Operator session confidentiality and integrity: protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure	✓	✓
		Vulnerability scanning: identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process	✓	✓
		Critical activity outsourcing: ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities	✓	✓
		Transaction business controls: restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business	✓	✓
	Physically secure the environment	Mandatory controls		
		Physical security: prevent unauthorized physical access to sensitive equipment, workplace environments, hosting sites and storage	✓	✓

[8] "Security controls: SWIFT issues core security standards and assurance framework for the community," Society for Worldwide Interbank Financial Telecommunications.

Objectives	Principles	Controls	Architecture A	Architecture B
Know and limit access	Prevent compromise of credentials	Mandatory controls		
		Password policy: ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy	✓	✓
		Multi-factor authentication: Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.	✓	✓
	Manage identities and segregate privileges	Mandatory controls		
		Logical access control: enforce the security principles of need-to-know access, least privilege and segregation of duties for operator accounts	✓	✓
		Token management: ensure the proper management, tracking and use of connected hardware authentication tokens (if tokens are used)	✓	✓
		Advisory controls		
		Personnel vetting process: ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting	✓	✓
		Physical and logical password storage: protect physically and logically recorded passwords	✓	✓
Detect and respond	Detect anomalous activity to systems or transaction records	Mandatory controls		
		Malware protection: ensure that local SWIFT infrastructure is protected against malware	✓	✓
		Software integrity: ensure the software integrity of the SWIFT-related applications	✓	
		Database integrity: ensure the integrity of the database records for the SWIFT messaging interface	✓	
		Logging and monitoring: record security events and detect anomalous actions and operations within the local SWIFT environment	✓	✓
		Advisory controls		
		Intrusion detection: detect and prevent anomalous network activity into and within the local SWIFT environment	✓	
	Plan for incident response and information sharing	Mandatory controls		
		Cyber incident response planning: ensure a consistent and effective approach for the management of cyber incidents	✓	✓
		Security training and awareness: ensure all staff are aware of and fulfill their security responsibilities by performing regular security training and awareness activities	✓	✓
		Advisory controls		
		Penetration testing: validate the operational security configuration and identify security gaps by performing penetration testing	✓	✓
		Scenario risk assessment: evaluate the risk and readiness of the organization based on plausible cyber attack scenarios	✓	✓

EY contacts

William Beer
+1 212 360 9010
william.beer@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

JB Rambaud
+1 212 773 4617
jb.rambaud@ey.com

Chris Kipphut
+1 704 338 0491
chris.kipphut1@ey.com

Jaime Kahan
+1 212 773 7755
jaime.kahan@ey.com

Roy Thetford
+1 212 773 3000
roy.thetford@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

Margaret Weichert
+1 404 817 4854
margaret.weichert@ey.com

Chris Lanzilotta
+1 410 783 3739
christopher.lanzilotta@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory 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. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace

Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2017 EYGM Limited.
All Rights Reserved.

EYG No. 01463-171Gbl
1702-2204587 BDFSO
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com