

SWIFT Customer Security Program

Time to get ready

Key dates

- ▶ End of Q1 2017: CSP standards finalized
- ▶ Start of Q2 2017: First annual self-attestation against 16 mandatory controls
- ▶ 1 January 2018: SWIFT starts enforcement, inspections and disclosures on non-compliance against the mandatory controls; customers can expand their disclosures to cover 11 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 6.1 billion transactions a year, of which a significant minority (around one-fifth) 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. Starting in the second quarter of 2017, SWIFT's customers will have to attest to complying with 16 mandatory controls. In January 2018, SWIFT will start sharing information on non-compliance with customers' regulators and counterparties and enforcing compliance by randomly selecting customers who will be required to provide additional information from their internal or 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
- ▶ Detailed knowledge of, and controls over, data flows linkages to business processes, and dependencies on external critical vendors

¹ Martin Arnold, “Swift outlines fightback against cyber theft,” 23 May, 2016, *Financial Times*

- ▶ 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 to 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: "Cyber-attacks 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 cybersecurity. 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 to 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 – 6.1 billion messages were sent through the system in 2015, or nearly 17 million a day.⁶ These transactions have a highly predictable format, so they're harder to protect.
- ▶ **Manual processing.** Over one-fifth of transactions still involve manual processing – that's more than 1.2 billion transactions a year. That rate hasn't changed much in the last few years.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 likely relegates SWIFT below other payment systems in its plan. Yet, the overall trend in cyber risk management is toward a three-lines-of-defense approach to addressing cyber risks.
- ▶ **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 controls and new technologies. Enhancements to SWIFT security have to leverage, and be combined with, these broader payments security upgrades.

² "SWIFT Customer Security Programme FACTSHEET," Society for Worldwide Interbank Financial Telecommunications

³ *Ibid.*

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

⁵ *Ibid.*

⁶ "About us," Society for Worldwide Interbank Financial Telecommunications

⁷ "Fund processing standardization: tracking industry progress," mid-2013, European Fund and Asset Management Association and Society for Worldwide Interbank Financial Telecommunications

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 audit 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 those 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:

- ▶ Build 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 aims to require certain 16 mandatory controls and encourage voluntary adoption of 11 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. 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., the *Framework for Improving Critical Infrastructure Cybersecurity* from the National Institute of Standards and Technology.

For each mandatory and advisory control, SWIFT has released so-called control statements, or definitions. It is consulting with industry on those statements and will publish final control statements by the end of the first quarter, 2017. The full set of objectives, principles and controls can be found in Table 1 on page 5.



The key implementation questions to be addressed

Implementation of SWIFT's CSP begins now. Customers have to self-attest to the mandatory controls in the second quarter of 2017.

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

- 1. Whether to adopt the advisory controls?** Customers have no choice but to implement the 16 mandatory controls, but they do have to determine whether to voluntarily adopt some or all of the 11 advisory controls. 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. Whether to 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 16 mandatory controls. Additionally, SWIFT customers can decide to conduct more stringent inspections to show compliance – including against the 11 advisory controls – through self-inspection, where certification is conducted by internal audit, or through a third-party inspection. 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 to disclose?** SWIFT will begin disclosing information to counterparties about customers' compliance with the advisory controls in January 2018. They will also start conducting inspections of sample customers, using internal and external audit⁸, to evaluate the quality of compliance, and enforcing compliance where quality is insufficient. 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 to engage the Chief Information Security Officer (CISO), risk professionals and others across the firm?** To be successful, firms should engage CISOs and second-line technology 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, legal, compliance and operational risk.
- 5. How to link SWIFT compliance to other cyber compliance 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 program. A siloed approach that treats all new requirements separately would 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 will 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 get surfaced, 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. The fact that the full final program is out for consultation between SWIFT, its customers, and other key regulators may support such an approach. However, that would be a mistake. SWIFT's CSP is demanding, and almost upon the industry. Acting now is critical.

⁸ Fund processing standardization: tracking industry progress," mid-2013, European Fund and Asset Management Association and Society for Worldwide Interbank Financial Telecommunications.

Table 1: SWIFT CSP control requirements⁹

Objectives	Principles	Controls
Secure your environment	Restrict internet access and segregate critical systems from general IT environment	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ SWIFT environment segregation: A segmented secure zone safeguards the local SWIFT environment from compromises and attacks from the broader enterprise and external environment. ▶ Operating system privileged account control: Access to local operating system accounts with system-level administrative rights is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, the accounts are restricted from being accessed.
	Reduce attack surface and vulnerabilities	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ Internal data flow security: Confidentiality, integrity and authentication mechanisms are implemented to protect SWIFT data flows within the secure zone, and its link to the user PCs. ▶ Security updates: All hardware and software inside the secure zone and on user PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied. ▶ System hardening: Security hardening is conducted on all systems and infrastructure within the secure zone and on the user PCs. <p>Advisory controls</p> <ul style="list-style-type: none"> ▶ Back office data flow security: Confidentiality, integrity, and authentication mechanisms are implemented to protect data flows between back office systems or middleware and the secure zone. ▶ External transmission data protection: Sensitive data leaving the secure zone is encrypted. ▶ User session integrity: The integrity and confidentiality of interactive user sessions connecting to the secure zone are safeguarded. ▶ Vulnerability scanning: Vulnerability scanning is conducted within the secure zone and on user PCs using an up-to-date industry-standard scanning tool. ▶ Critical activity outsourcing: Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organization. ▶ Transaction business controls: Restrict transaction submission and receipt to expected bounds of normal business.
	Physically secure the environment	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ Physical security: Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

⁹ "Security controls: SWIFT issues core security standards and assurance framework for the community," Society for Worldwide Interbank Financial Telecommunications

Objectives	Principles	Controls
Know and limit access	Prevent compromise of credentials	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ Password policy: All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. ▶ Multi-factor authentication: Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.
	Manage identities and segregate privileges	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ User account management: Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties. ▶ Token management: Authentication tokens are managed appropriately during issuance, revocation, use, and storage. <p>Advisory controls</p> <ul style="list-style-type: none"> ▶ Personnel vetting process: Staff operating the locally hosted SWIFT infrastructure are vetted prior to initial employment in that role and periodically thereafter. ▶ Physical and logical password storage: Any recorded passwords for privileged accounts are stored in a protected physical or logical location, with access restricted on a need-to-know basis.
Detect and respond	Detect anomalous activity to systems or transaction records	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ Malware protection: Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems. ▶ Software integrity: A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications. ▶ Database integrity: A database integrity check is performed at regular intervals on databases that record SWIFT transactions. ▶ Logging and monitoring: Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently review logs. <p>Advisory controls</p> <ul style="list-style-type: none"> ▶ Intrusion detection: Intrusion detection is implemented to detect unauthorized network access.
	Plan for incident response and information sharing	<p>Mandatory controls</p> <ul style="list-style-type: none"> ▶ Cyber incident response planning: The organization has a defined cyber incident response plan. ▶ Security training and awareness: Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access. <p>Advisory controls</p> <ul style="list-style-type: none"> ▶ Penetration testing: Application, host, and network penetration testing is conducted at least annually within the secure zone and on user PCs. ▶ Scenario risk assessment: Scenario-driven risk assessments are conducted regularly to improve incident response preparedness and to increase maturity of the organization's security program.

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

Jaime Kahan

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

Chris Kipphut

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

Chris Lanzilotta

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

Ertem Osmanoglu

+1 212 773 3520
ertem.osmanoglu@ey.com

JB Rambaud

+1 212 773 4617
jb.rambaud@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



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.