Wilson Consulting Group

Swift Assessment Security Services

Are you ready?

“Customers are individually responsible for the security of their own environments, however, the security of the industry as a whole is a shared responsibility.”

Society for Worldwide Interbank Financial Telecommunications (SWIFT)

What You Need To Know

The world is changing rapidly and cybercriminals are adapting to it more quickly, in some cases, than legitimate organizations. The growing network of connected devices in the Internet of Things (IoT) means businesses will be coping with a new class of attack vectors, from smart point-of-sale (POS) devices to flying drones. Also, targeted attacks by highly competent and persistent cybercriminals are now a fact of life for many organizations.

This has prompted The Society for Worldwide Interbank Financial Telecommunications (SWIFT) to take immediate action, even though customers are ultimately responsible for protecting their own environments. SWIFT’s Customer Security Program (CSP) was established to support customers in their fight against cyber-fraud.

SWIFT released a new Customer Security Control Framework (CSCF) for their Customer Security Program (CSP) on May 19, 2017. Financial institutions are now required to self-assess their SWIFT local environments against the new CSCF annually.

Based on their self-assessment results, institutions are required to submit a self-attestation on their compliance with the individual CSCF controls. This means that institutions will need to:

1. Outline the way in which their standard operating procedures align with the new SWIFT security objectives, principles, and controls
2. Document and report on this alignment to the SWIFT authorities

CRITICAL TAKEAWAYS:

✓ **On January 1, 2018, SWIFT** will begin enforcement, via inspections and disclosures, of businesses that are non-compliant with the new security standards.

✓ SWIFT requires all customers to submit an annual self-attestation and businesses that are found to be non-compliant will be reported to their customers, to regulators, and to other SWIFT members.

✓ **Wilson Consulting Group (WCG)** offers an assessment of your SWIFT financial processes, controls, and governance against the **SWIFT CSP Objectives, Principles, and Controls.**

✓ We provide expert advice and guidance on how to maintain a posture of compliance with the new SWIFT requirements which will prepare your organization **for the imminent January 1, 2018 enforcement deadline** and annual enforcements thereafter.

Contact WCG Today

Wilson Consulting Group, LLC

+1-866-780-1655 | sales@wilsoncgrp.com | wilsoncgrp.com | 800 Maine Avenue SW, Suite 200 Washington DC 20024

Wilson Consulting Group

What is SWIFT Customer Security Program (CSP)?

- The SWIFT Customer Security Program (CSP) is an initiative that was established to support customers in the fight against cyber-attacks. CSP aims to reinforce the security of the global financial system by improving the local security environment of each individual institution.
- Beginning in **the second quarter of 2017, all SWIFT customers** must attest, on an annual basis, that they: comply with 16 mandatory controls relevant to the security of their respective environments, have the knowledge and limitation of access to data, and are able to respond to cybersecurity threats. Institutions will also have the option to adopt 11 additional advisory controls.
- The SWIFT CSP requires each organization to define, document, implement, and assess their payment processes and technologies against SWIFT's set of **Objectives, Principles, and Controls.**

It is important to keep in mind the relationship between CSP and CSCF. The CSCF was developed as a framework to guide institutions on meeting the Customer Security Program objectives. To participate in SWIFT's Customer Security Program, institutions must meet the expectations of the security controls framework.

What is SWIFT Customer Security Control Framework (CSCF)?

Due to the growing risks in the global tech market mixed with the incredibly sensitive nature of content being relayed over networks, SWIFT requires financial institutions to provide detailed proof of compliance. The SWIFT Customer Security Controls Framework (CSCF) establishes the objectives, principles, and controls necessary to comply with baseline security requirements for the CSP.

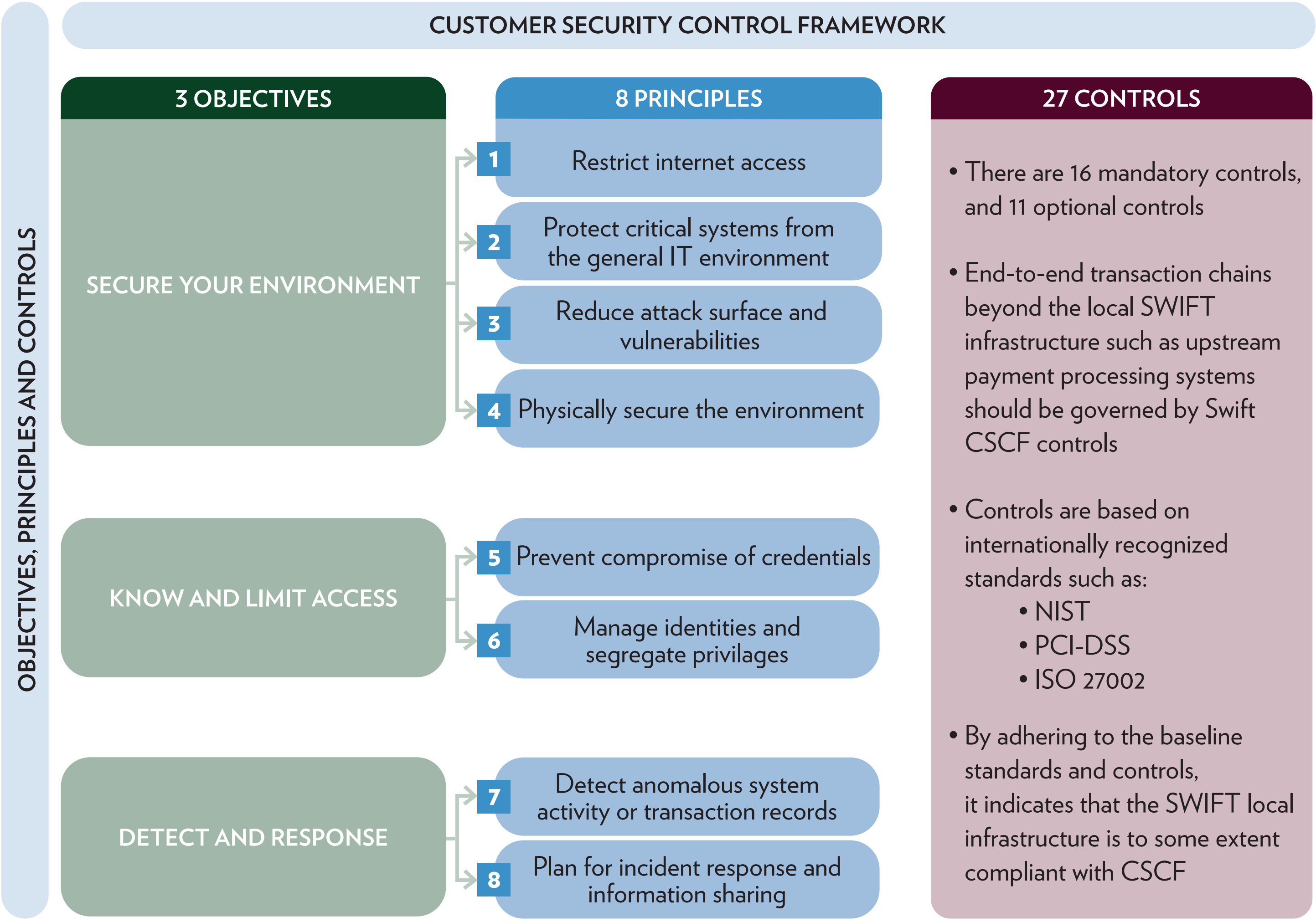
The CSCF describes a set of mandatory and advisory security controls for participating SWIFT institutions.
The mandatory security controls are utilized to ensure and maintain a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructures. SWIFT has chosen to prioritize these mandatory controls to set a realistic goal for near-term, tangible security gain and risk reduction.

All controls are articulated around three overarching objectives:

1. **Secure your Environment**
2. **Know and Limit Access**
3. **Detect and Respond**

- The controls have been developed based on SWIFT's analysis of cyber-threat intelligence and in conjunction with industry experts and user feedback.
- The control definitions are also intended to be in line with existing information security industry standards.
- Given the evolving nature of cyber-threats, institutions are to regularly assess the controls and to refine and expand them as necessary.
- To ensure adoption of the controls, SWIFT has developed an attestation and compliance process which will require participating institutions to self-attest compliance against the mandatory and, optionally, the advisory security controls.

The following is an illustration of the CSCF:



OBJECTIVES, PRINCIPLES AND CONTROLS

CUSTOMER SECURITY CONTROL FRAMEWORK

3 OBJECTIVES

SECURE YOUR ENVIRONMENT

KNOW AND LIMIT ACCESS

DETECT AND RESPONSE

8 PRINCIPLES

1 Restrict internet access

2 Protect critical systems from the general IT environment

3 Reduce attack surface and vulnerabilities

4 Physically secure the environment

5 Prevent compromise of credentials

6 Manage identities and segregate privilages

7 Detect anomalous system activity or transaction records

8 Plan for incident response and information sharing

27 CONTROLS

- There are 16 mandatory controls, and 11 optional controls
- End-to-end transaction chains beyond the local SWIFT infrastructure such as upstream payment processing systems should be governed by Swift CSCF controls
- Controls are based on internationally recognized standards such as:
  - NIST
  - PCI-DSS
  - ISO 27002
- By adhering to the baseline standards and controls, it indicates that the SWIFT local infrastructure is to some extent compliant with CSCF

Wilson Consulting Group

How Do You Become Compliant?

Wilson Consulting Group is ready to Help

SWIFT Assessment Security Services:

Wilson Consulting Group works with your organization to ensure that you meet the new SWIFT CSP Objectives, Principles, and Controls ahead of the **January 1, 2018 deadline**. Our SWIFT Assessment Security Services:

- Conduct **Gap Analysis** to review your organization's current security posture relating to your SWIFT Payment and Wire Transfer processes
- Conduct **Remediation** of all identified gaps to improve your organization's security posture
- Provide **Attestation services** to aid organizations in preparing for and executing the SWIFT CSP attestation which includes self-attestation, self-inspection, and **third party** inspection

What Makes WCG's Assessment

✓ Provides a compliance dashboard that shows your organization's overall compliance with the SWIFT CSP with mappings to PCI-DSS and ISO 27002 controls

✓ Ensures compliance between your policies, processes, and procedures with the SWIFT CSP Objectives, Principles, and Controls

✓ Utilizes unrivaled and "industry best" information gathering and assessment techniques and tools

✓ Develops progressive actionable plan for subsequent annual compliance

Financial Institutions Choose Us Because Of Our:

- Unparalleled experience aiding governments and businesses around the world in defending themselves against cybercrime, reducing their risks, complying with regulations, and transforming their IT and security operations and infrastructure
- Trusted leadership from experienced and highly qualified assessors
- Hands-on, interactive compliance guidance conducted by security experts who have extensive knowledge and experience helping institutions
- Ability to exceed industry requirements
- Exceptional reputation and track record
- Simple, straightforward pricing with no hidden agenda, charges, or add-on fees whatsoever
- Personable, dedicated staff to answer any questions you have at any time throughout the process

Contact WCG Today

Wilson Consulting Group, LLC

+1-866-780-1655 | sales@wilsoncgrp.com | wilsoncgrp.com | 800 Maine Avenue SW, Suite 200 Washington DC 20024