Secura

A BUREAU VERITAS COMPANY

CISO PRIORITY:

Critical Updates to the SWIFT Customer Security Programme

June 2021

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

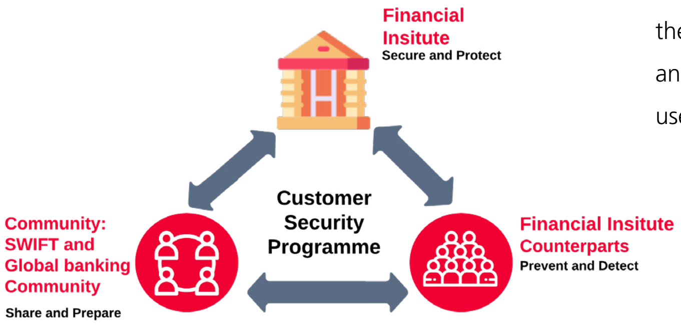
Follow us on

*The financial sector is one of the main targets for cyberattacks. The **SWIFT network (Society for Worldwide Interbank Financial Telecommunications)** and its clients have been the victim of such attacks over the past years resulting in large financial losses. Most notable is the Bangladesh Bank, where due a malware infection $81 million dollars was stolen from bank accounts. In response, SWIFT introduced the **Customer Security Program (CSP)** in 2016. In July 2019, SWIFT released the **Independent Assessment Framework (IAF)** indicating that, all SWIFT members have to perform an independent assessment based on Community Standard Assessments to improve the level of assurance and verification of the security controls implementation. Per 2021, all SWIFT users are required to ask an external party to perform an independent assessment to professionalise compliance with the mandatory controls of the Customer Security Controls Framework (CSCF v2021). This has to be set-up during the second half of 2021: are you ready for the new control and the external check?*

1. Basics of the Customer Security Programme (CSP)

All SWIFT connected parties are aware of the **Customer Security Programme (CSP).** SWIFT established the CSP to actively support customers in the fight against cyber-attacks in 2016. The CSP consists of three key focus areas:

- Securing the local SWIFT infrastructure and enforcing policies.
- Managing security risks in the interactions and relationships with banking counterparts by preventing and detecting fraud.
- Constantly sharing information and preparing for future cyber-attacks.


Financial Insitute
Secure and Protect
Customer Security Programme
Community: SWIFT and Global banking Community
Share and Prepare
Financial Insitute Counterparts
Prevent and Detect

This figure between an individual bank, their counterparts (business relationships and parts involved in SWIFT banking operations and messaging) and the bigger community (including SWIFT and the global banking network).

To support these goals, SWIFT introduced the **Customer Security Controls Framework (CSCF)**. The framework describes a set of mandatory and advisory security controls for SWIFT customers.

While all customers are responsible for protecting their own environment, the CSP improves information sharing within the community, enhances SWIFT-related tools for customers and provides a set of cybersecurity controls which helps users strengthen end-point security and combat cyber fraud.

2. Customer Security Controls Framework (CSCF) Structure

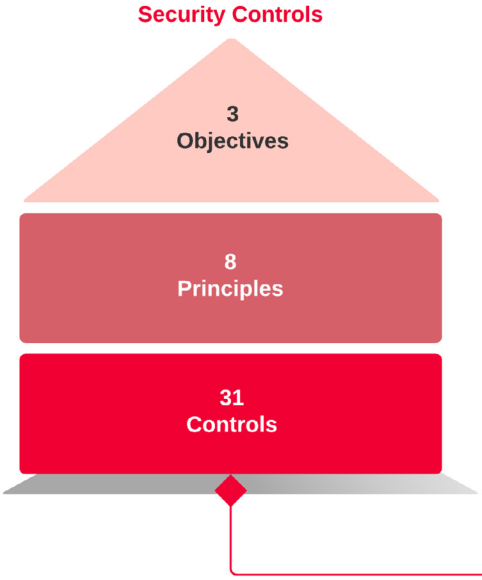
SWIFT set up the CSCF Structure to reinforce the security of the global banking system. The SWIFT Customer Security Controls are articulated around three overarching objectives:

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

These are defined by the 8 principles shown below and detailed in 31 controls. The CSCF v2021 is currently composed of 22 mandatory and 9 advisory controls.

For the organizations using the SWIFT infrastructure and SWIFT payment gateway, SWIFT demands compliance with the controls defined in the SWIFT CSC framework.

The compliance with the controls need to be demonstrated at the end of each calendar year. Therefore, end of 2021 for the current version of the controls framework.



Security Controls

3 Objectives

8 Principles

31 Controls

CSP Security Controls Framework

Security Your Environment	1.* Restrict internet access
	2.* Segregate critical systems from general IT environment
	3. Reduce attack surface and vulnerabilities
	4. Physically secure the environment
Know and Limit Access	5. Prevent compromise of credentials
	6. Manage identities and segregate priviliges
Detect and Respond	7. Detect anomalous activity to system or transaction records
	8. Plan for incident response and information sharing

* 1 & 2 are combined in the CSCF

- **Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure.**
- **Consists of 22 mandatory and 9 advisory controls**
- **Independent assessment: SWIFT require all customers to undergo an independent assessment to support their self-attestation against CSFC v2021.**
- **Full Compliance against mandatory controls by the end of 2021**

3. Key Changes in the 2021 CSCF

With the last change in 2019, the 2021 version has a few important updates of which the mandatory attestation is the most important. Key changes compared to the CSCF v2021 version include:

1. **A new architecture type is included (A4)**
   This newly introduced architecture type covers customers with non-SWIFT footprint. It consists of using customer connectors (middleware servers or API endpoints) to directly connect and interface with SWIFT services.
2. **Emphasis on risk-based approach**
   Through a risk-based approach previously unknown factors can be identified by prioritizing security controls.
3. **Third-party engagement extensions to cloud provider**
   With more and more companies moving to the cloud, SWIFT provided third-party engagement extensions to cloud providers to enhance security for these solutions.
4. **Shared responsibilities illustration specific to IaaS cloud model**
   To highlight and explain how responsibility is seen, SWIFT shared an IaaS cloud model with assigned responsibilities as an example.
5. **Vulnerability scanning is mandatory**
   With the amount of attacks increasing, vulnerability scanning is now officially mandatory (except for architecture B where it is advised).

SWIFT Deployment Types

SWIFT architecture types are reference architectures that users choose from as the closest representation of their environment. These architecture types also determine the applicability and scope of CSCF controls. SWIFT provides its customers with five possible application diagrams for their SWIFT deployment.

- For organizations that run most or all of their SWIFT functionality themselves (architectures A1, A2, A3 and A4), mapping the extent of their SWIFT infrastructure is critical.
- Architecture B applies when an organizations outsources most of its SWIFT functionality. This means that most critical systems reside on an external network that is beyond their immediate control.

4. Key Milestones for Your 2021 CSP Assessment

As the CSP requires, SWIFT users should perform an annual assessment of their security environment against the CSCF requirements. They would then need to follow up by providing their self-attestation of their compliance status against the CSCF mandatory controls via the KYC Registry Security Attestation Application.

The self-attestation based on Community Standard Assessment is mandatory as of 2021.

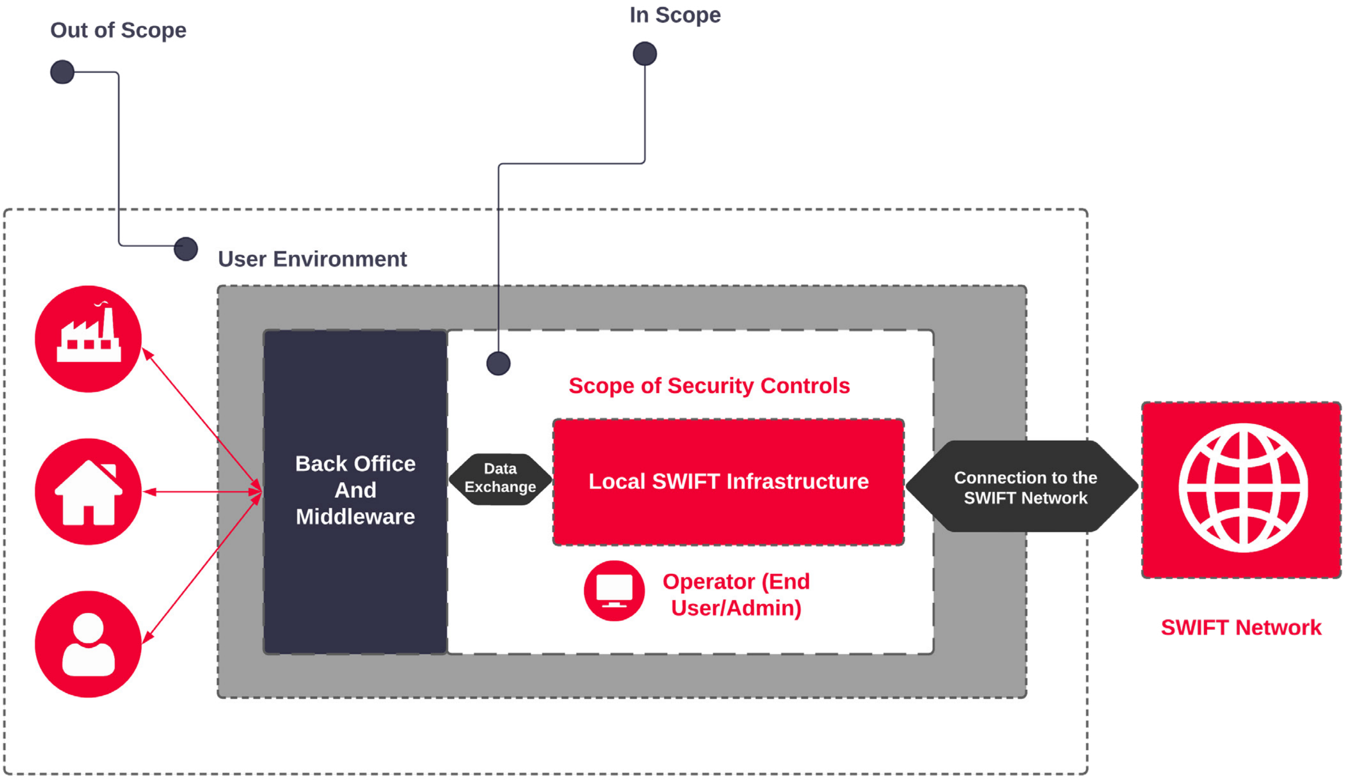
The Community Standard Assessment is an assessment by an independent third party or the organization's internal compliance, internal risk or internal audit departments, if this exists within the organization. Larger organizations sometimes have independent internal audit departments, while smaller financial institutions often do not have completely separated audit teams. For these companies it is key to prepare this process well.

5. How to Scope Your SWIFT CSP Assessment?

Performing the SWIFT CSP assessment and deriving the associated self-attestation requires in the first place that the organizations execute the testing and validation procedures in line with the controls highlighted in the SWIFT CSCF. Some of the controls defined in the SWIFT CSCF can be validated either by the means of penetration testing on the target SWIFT Infrastructure. Others can be assessed from an audit perspective, by the validation of successful alignment of controls with the SWIFT CSP guidelines resulting in a controls-based report.

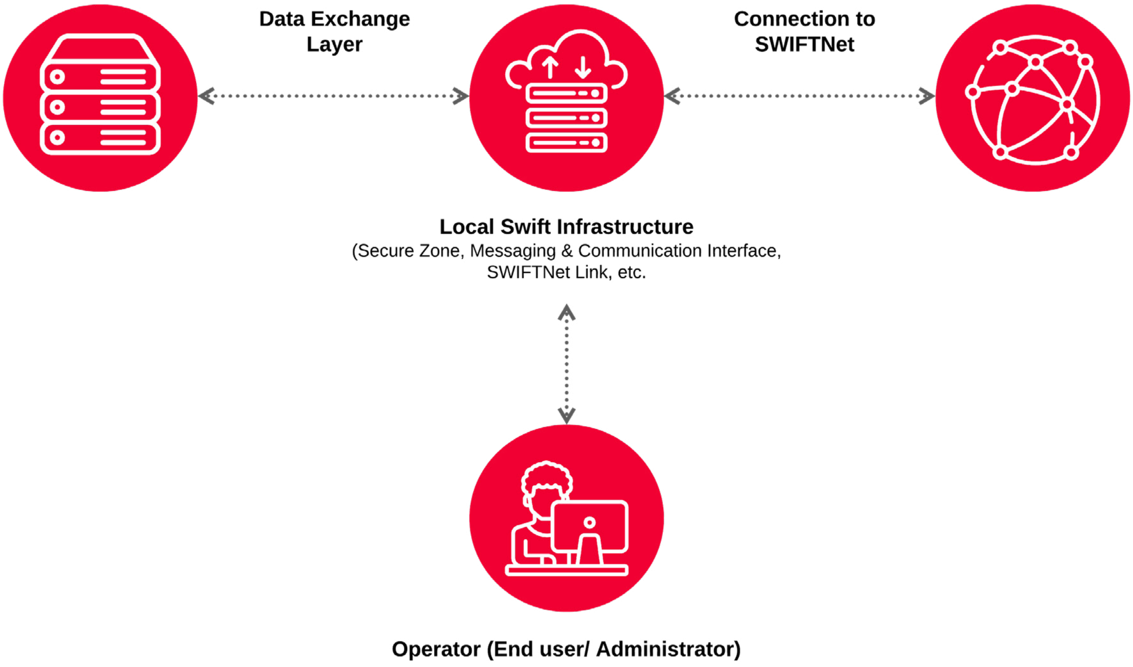
Scope of SWIFT Security Controls

When determining the scope of SWIFT security controls it is helpful to understand the generic architecture of SWIFT infrastructure. Here, you see the **general banking environment** (user environment) with **Back office** and **middleware** with a **Data exchange connection** to the **Local Swift Infrastructure**, which connects to the **general SWIFT network**. The local SWIFT infrastructure is managed by the **Operator** (end user/admin), who works on specific **Operators PC**.


Out of Scope
In Scope
User Environment
Back Office And Middleware
Data Exchange
Scope of Security Controls
Local SWIFT Infrastructure
Operator (End User/Admin)
Connection to the SWIFT Network
SWIFT Network

The following list contains the scope of the SWIFT security assessment:

- **Data exchange layer**: The flow of data between the back office (or middleware layer) and the SWIFT infrastructure.
- **SWIFT Local Customer Infrastructure**: SWIFT-specific components managed or owned by an organization, including:
    - SWIFT Messaging Interface
    - Communication interface
    - SWIFTNet Link (SNL):
        - Single-Window access to SWIFT
        - Mandatory software for interoperability ensuring integrity, authentication and confidentiality.
    - Connector
    - SWIFT HSMSs
    - Secure Zone
- **SWIFT operator's machines**: The end user or administrative computing device (typically a desktop or laptop) used to operate or maintain the local SWIFT infrastructure. If jump hosts are implemented it is also part of the scope.
- **Operators**: Operators are individual end users and administrators who interact directly with the local SWIFT infrastructure.


Data Exchange Layer
Connection to SWIFTNet
Local Swift Infrastructure
(Secure Zone, Messaging & Communication Interface, SWIFTNet Link, etc.
Operator (End user/ Administrator)

6. SWIFT CSP Assessment Approach

Companies using SWIFT infrastructure must comply with new security requirements. Compliance typically involves an assessment approach. For these assessments, Secura follows the following step-by-step approach, designed for maximizing the work efficiency and ensure a seamless execution. A gap assessment is performed to fully understand the current situation and evaluate it against the SWIFT CSP objectives, processes, and controls. A timely remediation plan for the identified gaps will make sure your future situation corresponds to the required SWIFT CSP objectives. Additionally, this will help to prevent disclosing any non-compliant controls in the independent assessment.

Our approach for a SWIFT security assessment consists of four steps: preparation, a threat modeling session, followed by the execution of the assessment activities, and reporting of the findings.

1. PHASE 1: Work Preparation

Determing a complete overview of the SWIFT infrastructure, target scope, and the implemented processes and procedures.

2. PHASE 2: Threat Modeling / Risk Assessment

Detailed threat modeling according to STRIDE methodology to support the risk-based approach and to jointly assess if new risks/threats can be identified.

3. PHASE 3: Technical Assessment & Audit Assessment of the technical SWIFT controls

3.1. Penetration Testing on applicable SWIFT controls
3.2. Black box infrastructure assessment
3.3. Mapping of tests to the SWIFT CSCF

Audit for applicable process-related SWIFT CSP controls

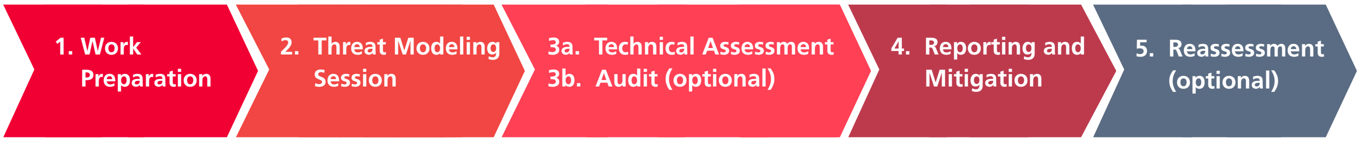
Two types of CSP security controls can be covered by this audit:

a. Security controls, which are partially covered by the penetration testing on the technical features. For these controls, the process and procedures behind the deployment of the features are assessed.
b. Security controls which can be validated by assessing the processes and procedures. For these controls, the existence and correct/complete implementation of the processes and procedures are reviewed.

4. PHASE 4: Reporting and mitigation

In this phase, the information gathered during the assessment is analyzed, reviewed and reported. This report will include evidences, a gap analysis, and recommendations to achieve a compliant state.

The SWIFT CSP audit service, focused on the process-related SWIFT controls, will provide a complementary approach to the penetration testing activities. The process-related findings will be further compiled into the audit report, together with the relevant findings of the penetration testing activity.
The goal of the SWIFT CSP assessment is to validate the process behind the way in which the controls are implemented, the internal documents supporting the implementation of the process (e.g. internal policies related to a specific process), and evidence that the process is followed (e.g. logging of various process steps or taken actions). This provides financial institutions with a clear overview and input for their CSP assessment.


1. Work Preparation
2. Threat Modeling Session
3a. Technical Assessment
3b. Audit (optional)
4. Reporting and Mitigation
5. Reassessment (optional)

What happens if you are not compliant?

SWIFT enforces compliance through the community by peer awareness and data for companies to make decisions of potential risk of counterparts. Banking-related penalties can be enforced, but are not controlled by SWIFT.

Self-Attestations

If members are not CSCF compliant or don't submit self-attestations, their status is visible to the SWIFT community and any member can determine their status.

Transactions

If parties that do transactions are not compliant, SWIFT will inform counterparties and their ability to transact business and facilitate payments will be limited.

The Standards MT Release 2020

Financial Action Task Force (FATF-16) can impose penalties or sanctions for breaches. Rules may include unlimited fines for companies, and could mean prison for key individuals.

Bank Penalties

Reserve Bank of India imposed penalties on 36 banks for non-compliance.

7. How Secura Helps Meeting the SWIFT Assessment Requirements?

- **SWIFT CSP Audit**

  Audit and validation of successful compliance alignment of controls with the SWIFT CSP guidelines resulting in a controls report under recognised standards (e.g. ISAE3000).

- **SWIFT CSP Assessment**

  A detailed assessment from an audit perspective of SWIFT CSP controls. This could be combined with a CSP audit.

- **Penetration Testing (VAPT)**

  Secura’s security experts can perform a thorough SWIFT infrastructure assessment.

- **Adapting to your requirements**

  Secura will leverage its extensive SWIFT CSP expertise to ensure that your needs are met ahead of SWIFT's required independent assessment due on 31 December 2021.

About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: **secura.com.**

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: www.secura.com/subscribe.

Follow us on

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS 1828

BUREAU

VERITAS

Shaping a World of Trust