Deloitte.

SWIFT Customer Security Programme

Independent Assessment
Attest Your Level of Compliance

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

The payment industry is confronted with the full spectrum of Cyber-Risks. While payment related Cyber Risks have been historically focused on fraud, they are not the only threat it faces from Cyber-attacks. Today the attacks on financial institutions are more sophisticated, advanced, and are executed with more complexity, the gains are also much higher. This creates a shift from focusing on large groups of customers to larger individual institutions.

SWIFT and What it does

Banks are connected to each other, creating a strong need for ensure communication between them. To ensure standardized financial messaging exchanges in a secure way, SWIFT developed a messaging platform. Today, over 11,000 customers in over 200 countries and territories are connected to the messaging platform, products, and services of SWIFT transferring more 31.3 million messages a day.

The 2024 SWIFT CSP Update and its Impact

SWIFT has introduced the Customer Security Programme (CSP) as a countermeasure to these Cybercrimes. However, it was also implemented to raise the bar of logical and physical security for the community.

Based on our experience with the evaluation of the CSCF at several SWIFT customers, we will analyze SWIFT-related breaches and the most common control failures in this document. We will also provide a set of recommendations on how to prepare for the self-attestation and how to secure your environment better.

Submit an attestation annually

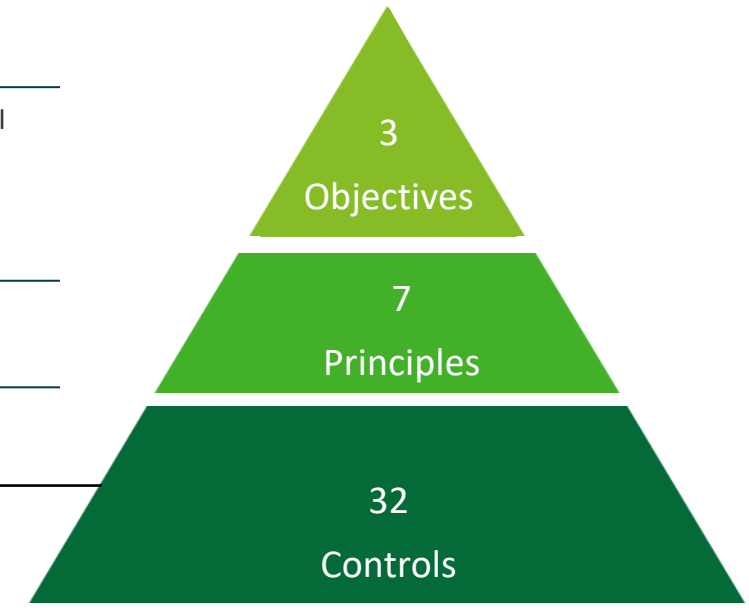
All users must attest before the expiry date of the current controls' version, confirming full compliance with the mandatory security controls no later than 31 December, and must re-attest at least annually thereafter. Re-attestation must be done between July and December each year. New joiners need to attest before going live on the Swift network.
The SWIFT Independent Assessment Framework (IAF), requires all Swift users must perform a Community Standard Assessment to further enhance the accuracy of their attestations. Swift mandates that the attestations submitted are **independently assessed**.

SWIFT CSP Objectives, Principles and Controls

The 2024 Customer Security Control Framework (CSCF) consists of a set of **3 objectives**, which focus on **7 principles** and contain **32 controls**.

The framework is applicable to five types of SWIFT user architectures, titled A1, A2, A3, A4 and B. SWIFT users must first identify which architecture applies to them before implementing the applicable controls.

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

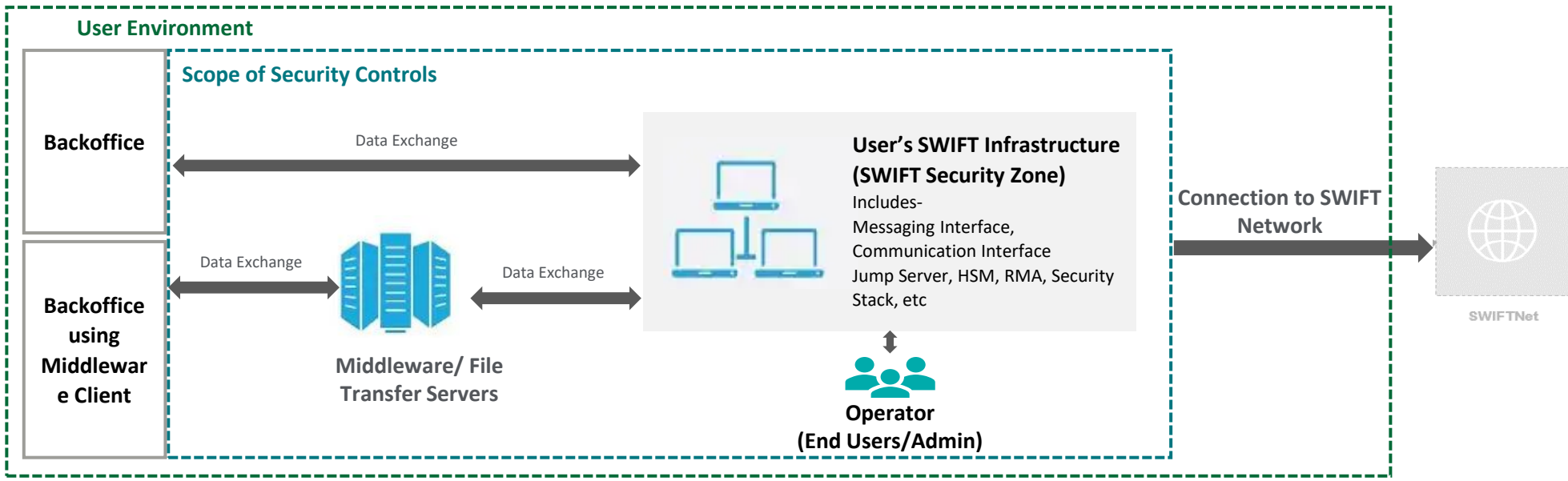


Fully compliance against mandatory controls expected by end of 2024

SWIFT CSP Assessment Scope

The below diagram depicts the scope of the Customer Security Control Framework (CSCF). The scope of the security control is applicable to a defined set of components in the user's local environment as depicted below. The scope may vary in size depending on the Architecture Type.

The objective is to establish controls and processes around the organization's SWIFT environment and infrastructure using a Risk-Based approach i.e assessing security goals, regardless of implementation. This will include an assessment of the control design and a point-in-time evaluation of the operational effectiveness.



Deloitte's Assessment Methodology

We have developed a tailor-made methodology based on SWIFT CSCF and international Cyber security standards specific for these type of engagements. We will provide services to deliver the insights related your compliance level based on CSCF specific know-how.

The below approach illustrates the collaborative approach and involvement of both parties during each broad step of the process.

Your Environment

Existing Business and IT environment

Collaboration with key stakeholders (business and IT) and advanced preparation including review of available relevant policies and procedures, including security environment, network architecture diagrams and evidence of control implementation.

+

The Deloitte's Approach

Assessment against SWIFT CSCF control objectives (not implementation guidelines checklist exercise)

Specifically developed Deloitte SWIFT CSCF methodology with focus on SWIFT perimeter and relevant components as stated in CSCF.

Professionals with 5+ experience in assessments against CSCF.

=

Outcomes

User Environment specific Independent Assessment

Our service will produce the following deliverable:

- Assessment results.
- Completion Letter (as defined by SWIFT).
- Management executive summary highlighting the scope, critical findings and the positive security aspects identified.

SWIFT CSCF Framework

The SWIFT CSCF Framework consist of 32 security controls (25 mandatory controls and 7 advisory controls) and underpin the objectives and principles where the first two principles, sharing common controls, have been grouped. The controls help mitigate specific Cyber-security risks that SWIFT users face due to the Cyber-threat landscape.

SWIFT CSP 2024

32 controls

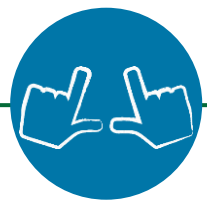
SWIFT CSP Controls

25 Mandatory controls					**7 Advisory controls**	
1.1 SWIFT Environment Protection	1.2 Operating System Privileged Account Control	1.3 Virtualisation or Cloud Platform Protection	1.4 Restriction of Internet Access	1.5 Customer Environment Protection	2.4A Back Office Data Flow Security	2.5A External Transmission Data Protection
2.1 Internal Data Flow Security	2.2 Security Updates	2.3 System Hardening	2.6 Operator Session Confidentiality and Integrity	2.7 Vulnerability Scanning	2.11A RMA Business Controls	5.3A Staff Screening Process
2.8 Outsourced Critical Activity Protection	2.9 Transaction Business Controls	2.10 Application Hardening	3.1 Physical Security	4.1 Password Policy	6.5A Intrusion Detection	7.3A Penetration Testing
4.2 Multi-Factor Authentication	5.1 Logical Access Control	5.2 Token Management	5.4 Password Repository Protection	6.1 Malware Protection	7.4A Scenario-based Risk Assessment	
6.2 Software Integrity	6.3 Database Integrity	6.4 Logging and Monitoring	7.1 Cyber Incident Response Planning	7.2 Security Training and Awareness		

SWIFT CSCF Framework

A Glance At The SWIFT CSP Changes

The SWIFT CSP changes are a continuous approach to defend against attacks and fraudulent activities connected to the financial scope. Below is the timeline of the changes over the years-



CSCF 2017	CSCF 2018	CSCF 2019	CSCF 2020	CSCF 2021	CSCF 2022	CSCF 2023	CSCF 2024
27 Controls	27 Controls	29 Controls	No Changes	31 Controls	32 Controls	32 Controls	32 Controls
16 Mandatory	16 Mandatory	19 Mandatory		22 Mandatory	13 Mandatory	24 Mandatory	25 Mandatory
11 Advisory	11 Advisory	10 Advisory		9 Advisory	9 Advisory	8 Advisory	7 Advisory

SWIFT's CSCF v2024 introduces few new requirements, namely:

1. New 'mandatory' control

2.8 Outsourced Critical Activity Protection

This set of controls, which focuses on ensuring that no new weaknesses or vulnerabilities are introduced when critical activities are outsourced to third parties or service providers, has been renamed and promoted to mandatory in CSCF v2024.

2. Significant 'advisory' scope increase

2.4A Back Office Data Flow Security

To support a phased promotion to mandatory, the scope of this control has been increased to properly identify:

- the servers bridging the back office and the user's secure zone
- the mechanisms securing the data flow exchange, either by end-to-end data protection or by securing each flow segment and the supporting 'bridging servers' which are guardians of such data exchange.

While the control 2.4A remains advisory, Swift recommends to already identify these flows and assess their security posture.

3. Other scope changes added as 'mandatory'

2.3 System Hardening – The scope of this control has been increased to include guidance related to USB ports protection fully. In addition, the optional enhancement related to application allowlisting has been moved from controls 1.1, 1.5 and 6.2 to control 2.3.

2.9 Transaction Business Controls – The control now explicitly mentions business controls can be performed outside the secure zone.

3.1 Physical Security – The scope of this control has been increased to encompass recommendations on reasonable sanitisation of disposed or reassigned equipment. In addition, wording regarding supervision and secure storing of tokens has been aligned in control 3.1 and 5.2.

7.4 Scenario-based Risk Assessment – The control now explicitly mentions reliance can be made on existing Information Security Risk Management processes.

4. Consistency updates, clarifications, and other changes

Several updates, clarification, and other changes were introduced to controls, including 2.1 Internal Data Flow Security, 2.2 Security Updates, 2.4 Back Office Data Flow Security, 3.1 Physical Security, 5.2 Token Management, 5.4 Password Repository Protection, and 6.2 Software integrity, 6.4 Logging and Monitoring, Appendix D, Appendix E, and Appendix F.

SWIFT CSP Assessment

Why Deloitte?

Deloitte's Cyber Risk practice is widely acknowledged as a leading security consulting practice and is eminently qualified to help your organization remain secure, vigilant, and resilient in the face of evolving Cyber threats.

- Deloitte has been acknowledged within the SWIFT CSP Certified Assessors Directory, having met specific eligibility criteria for assessment providers. We boast a SWIFT community group with 220+ professionals across the globe, including SWIFT CSP Certified Assessors.
- We have established a SWIFT Center of Excellence in Belgium which directly interfaces with SWIFT for new changes and enhancements. Our Team is provided with periodic trainings for SWIFT Assessments where SWIFT Architectures, control implementations, new enhancements provided by SWIFT are discussed.
- Deloitte's leadership in the field of information security assures you of our ability to assign qualified, knowledgeable, and industry-respected personnel who have performed similar consulting assignments
- Our experience in delivering similar mandates for local organizations brings industry specific experience. Our local industry resources and high experience of security technologies, constitute an invaluable set of resources for SWIFT CSP-related engagements. This enables us to use proven tools and methods to carry out comprehensive engagements
- We are a technology and solution agnostic, and we only recommend a solution that makes sense for the business and provides value

Case Study

The Challenge

The client, a Major Financial Institution in Middle East, wanted to review and strengthen the cyber security posture of its SWIFT environment. This project required to conduct an assessment against SWIFT CSCF covering people, process and technology dimensions.

The client was performing an independant SWIFT CSCF assessment for the first time, prior to this self- assessment were performed.

Our Approach

In order to deliver the highest quality of service, Deliotte's approach included:

- Guiding the client through the Self-attestation process by- leading **CSP workshops with key staff** both business and technical that are involved in the SWIFT self-attestation; checking system configurations and documentation; reviewing the SWIFT environment based on the SWIFT Customer Security Control Framework; highlighting deficiencies as soon as they are identified.
- Deloitte leveraged its established **SWIFT CSP Center Of Excellence in Belgium** with a professionals skilled and experienced in security projects based on SWIFT Customer Security Controls Framework (CSCF). The COE has liaison with SWIFT for updates and trainings.
- Our experts executed the projects from start to end, as subject matter experts in delivering the security assessments based on CSCF. Key gaps were identified in the infrastructure which was not identified in the past.
- In result, we delivered a **management report** useful for the self-attestation, this also included recommendations for remediation activities. Our numerous international experience and deep understanding of SWIFT requirements and controls, helped us suggest the most efficient remediation plans. We worked closely with the client key stakeholders in order to define a well-suited plan and close the gaps against SWIFT CSCF.

Contact us

Simon Chandran

Middle East FSI Cyber Leader

simonchandran@deloitte.com

+971 502041127

Vishwanath Nemani

Middle East FSI Director

vinemani@deloitte.com

+971 526244700

Deloitte.