Deloitte.

SWIFT Customer Security Program

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 than 8.4 billion FIN messages till date.

The 2023 SWIFT CSP Update and its Impact

SWIFT has introduced the Customer Security Program (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

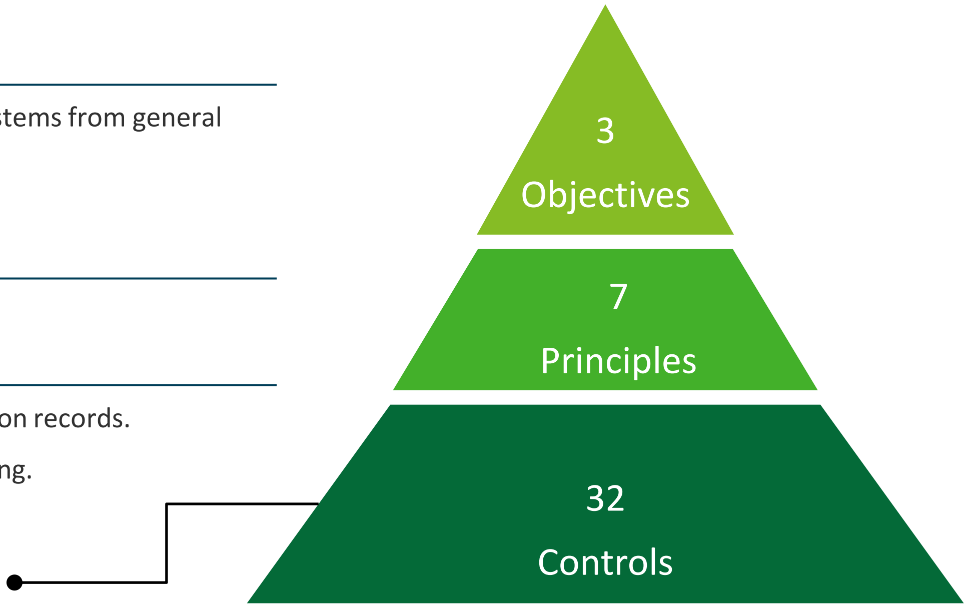
All users must attest before the expiry date of the current controls' version, confirming full compliance with the mandatory security controls no later than 31 December, and must re-attest at least annually thereafter. Re-attestation must be done between July and December each year. New joiners need 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 2023 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.

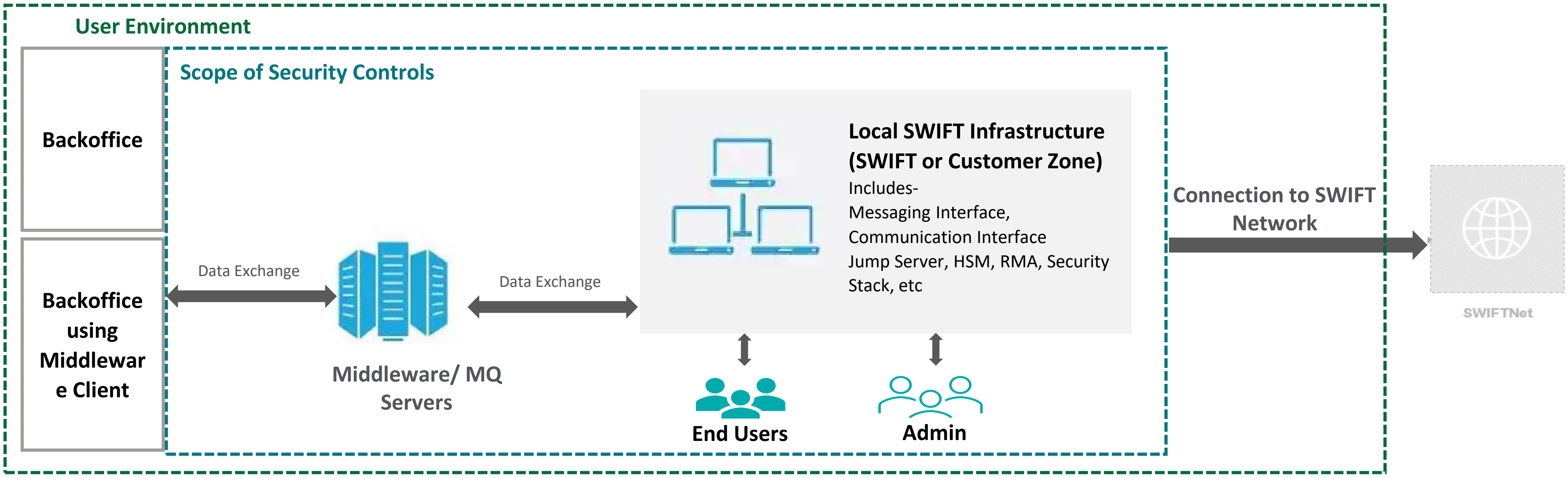


Fully compliance against mandatory controls expected by end of 2023

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.



User Environment

Scope of Security Controls

Backoffice

Backoffice using Middlewar e Client

Data Exchange

Middleware/ MQ Servers

Data Exchange

Local SWIFT Infrastructure (SWIFT or Customer Zone)

Includes-
Messaging Interface,
Communication Interface
Jump Server, HSM, RMA, Security Stack, etc

End Users

Admin

Connection to SWIFT Network

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

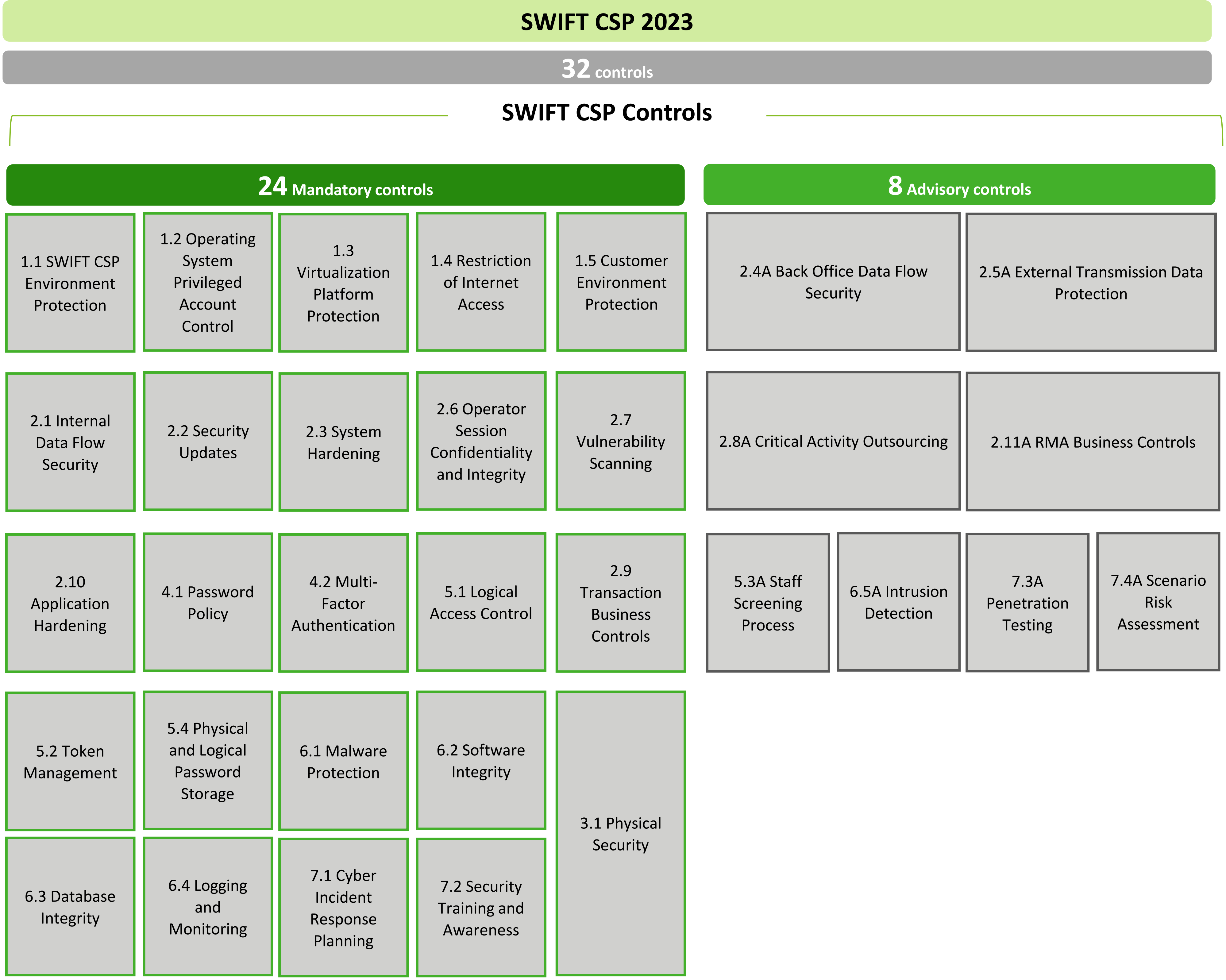
User Environment specific Independent Assessment

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 (24 mandatory controls and 8 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 2023

32 controls

SWIFT CSP Controls

24 Mandatory controls

1.1 SWIFT CSP Environment Protection

1.2 Operating System Privileged Account Control

1.3 Virtualization Platform Protection

1.4 Restriction of Internet Access

1.5 Customer Environment 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

2.10 Application Hardening

4.1 Password Policy

4.2 Multi-Factor Authentication

5.1 Logical Access Control

2.9 Transaction Business Controls

5.2 Token Management

5.4 Physical and Logical Password Storage

6.1 Malware Protection

6.2 Software Integrity

3.1 Physical Security

6.3 Database Integrity

6.4 Logging and Monitoring

7.1 Cyber Incident Response Planning

7.2 Security Training and Awareness

8 Advisory controls

2.4A Back Office Data Flow Security

2.5A External Transmission Data Protection

2.8A Critical Activity Outsourcing

2.11A RMA Business Controls

5.3A Staff Screening Process

6.5A Intrusion Detection

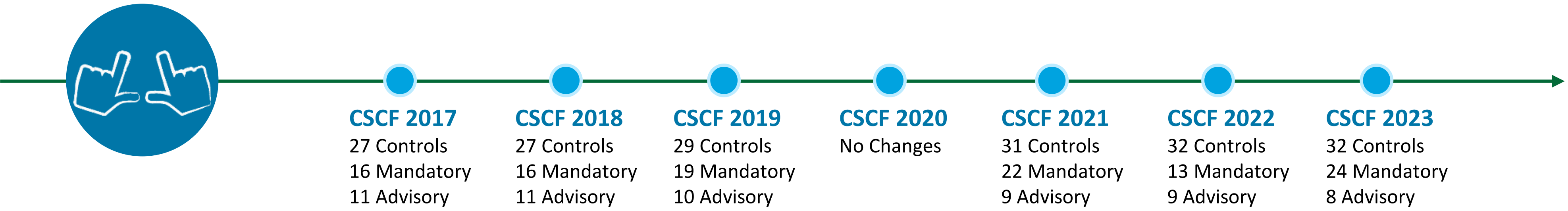
7.3A Penetration Testing

7.4A Scenario Risk Assessment

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
27 Controls
16 Mandatory
11 Advisory

CSCF 2018
27 Controls
16 Mandatory
11 Advisory

CSCF 2019
29 Controls
19 Mandatory
10 Advisory

CSCF 2020
No Changes

CSCF 2021
31 Controls
22 Mandatory
9 Advisory

CSCF 2022
32 Controls
13 Mandatory
9 Advisory

CSCF 2023
32 Controls
24 Mandatory
8 Advisory

SWIFT's CSCF v2023 introduces few new requirements, namely:

1. New 'mandatory' control

2.9 Transaction Business Controls
This set of controls, which focuses on detecting and preventing fraudulent outbound transaction activities, has become mandatory in CSCF v2022. The new requirements steer businesses to ensure SWIFT transactions are limited to those that support business as usual activities, and to restrict SWIFT transactions outside of customer-defined amount limits.

2. New 'advisory' control

1.5A Customer Environment Protection
This new control, which focuses mainly on the A4 architecture type, has the objective to strengthen the security of file transfer solutions or middleware systems, called customer connectors, used for SWIFT communication, by ensuring such communication take place within customer secure zones. This is a new advisory control that will become mandatory in the CSCF v2023.

3. Significant 'mandatory' scope increase for A4 architecture

Customer connector is now a mandatory component for A4 architecture type. There is a significant number of controls (i.e., 1.2, 1.3, 1.4, 2.2, 2.3, 2.6, 2.7, 3.1, 4.1, 4.2, 5.1, 5.4, 6.1, and 6.4) that need to be assessed for customer connector application level and underlying operating system and virtual platform to ensure fulfilment of the relevant controls' objectives.

4. Other scope changes added as 'mandatory'

1.2 Operating System Privileged Account Control
The scope of this control has been increased to restrict access to administrator-level operating system accounts defined in dedicated operator PCs and network devices, protecting the secure zone.

5. Other scope changes added as 'advisory'

1.2 Operating System Privileged Account Control- The scope of this control has been increased to restrict access to administrator-level operating system accounts defined in general-purpose operator PCs for all architectures.
6.2 Software Integrity and 6.3 Database Integrity- The scope of this control has been increased to ensure the software and database integrity.

6. Consistency updates, clarifications, and other changes

Several updates, clarification, and other changes were introduced to controls, including 1.2 Operating System Privileged Account Control, 2.1 Internal Data Flow Security, 2.6 Operator Session Confidentiality and Integrity, 4.2 Multi-Factor Authentication, 5.1 Logical Access Control, 5.4 Physical and Logical Password Storage, and 7.2 Security Training and Awareness.

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 ranked #1 by Gartner in security consulting services for the 7th consecutive year

- 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, Deloitte'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

Fadi Mutlak

KSA Cyber Leader

fmutlak@deloitte.com

+966 553629996

Ziad Haddad

UAE Cyber Leader

zhaddad@deloitte.com

+971 552542548

Tamer Charife

KQB Cyber Leader

tcharife@deloitte.com

+965 97314314

Deloitte.

This document has been prepared Deloitte & Touche (M.E.). for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Deloitte & Touche (M.E.). to supply the proposed services. This document and its contents are confidential and prepared solely for your information to allow you to assess if you would like to engage Deloitte & Touche (M.E.). in a formal contractual relationship, for the proposed service. This proposal should not be reproduced, redistributed or passed on directly or indirectly, to any other person or party, in whole or in part. Therefore, you should not refer to or use our name or this document for any other purpose, disclose it or refer to it in another document, or make it available or communicate it to any other party. In any event, no other party is entitled to rely on our documentation for any purpose whatsoever and thus we accept no liability to any other party who sees or gains access to this document. This document is not contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss the contractual terms and conditions with you prior to our appointment. Deloitte & Touche (M.E.) LLP (DME) is the affiliate for the territories of the Middle East and Cyprus of Deloitte NSE LLP (NSE ””), a UK limited liability partnership and member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities. DTTL (also referred to as Deloitte Global ””) and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see www.deloitte.com/about to learn more. Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories, serves four out of five Fortune Global 500 ® companies. Learn how Deloitte s approximately 410 ,000 people make an impact that matters at www.deloitte.com DME is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926 DME s presence in the Middle East region is established through its affiliated independent legal entities , which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME s affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.