AMR Cyber Security

# **Enhancing Cybersecurity in the Financial Industry**: A Comprehensive Guide to Swift Customer Security Programme (CSP)

DATE: January 2025

VERSION: 1.1

## TABLE OF CONTENTS

## Introduction

In an era of rapid technological advancements, the financial industry has witnessed a significant transformation in transactions and communications.

One of the key players in this landscape is the Society for Worldwide Interbank Financial Telecommunication (Swift), which facilitates secure and standardised messaging services for financial institutions worldwide. As the financial sector becomes increasingly interconnected and reliant on technology, the need for robust cybersecurity measures has never been more paramount.

This white paper aims to provide a comprehensive overview of the Swift Customer Security Programme (CSP), delving into the industry context, potential threats faced by the financial sector, the requirements for implementing the CSP, an exploration of the Swift Customer Security Controls Framework (CSCF), the approach to compliance and the methodology we employ to assist our valued customers.

Additionally, the paper will demonstrate how the CSP aligns with established cybersecurity frameworks such as NIST and ISO 27001, highlighting the benefits of partnering with us to enhance cybersecurity posture.

## Industry Context and Threats Facing Swift Customers

The financial sector has become a prime target for cybercriminals, due to the potential for monetary gain and for the opportunity to disrupt global economic stability. Attacks targeting financial institutions range from data breaches to ransomware attacks, with attackers exploiting network vulnerabilities, systems, applications and people. The interconnected nature of the financial ecosystem amplifies the impact of such attacks, making it imperative for organisations to protect themselves via in-depth, layered defences. It is not just criminal groups that are targeting the financial sector. Nation-state actors have also reportedly been targeting financial institutions and operators. Programmes such as the CSP are vital in securing the financial sector because of these highly capable threat actors.

In 2015 and 2016, the threat actor known as the Lazurus Group carried out a set of attacks on Bangladesh Central Bank and then a commercial bank in Vietnam. Exploiting vulnerabilities within Swift's network, the Lazurus Group issued unauthorised Swift messages and attempted to steal almost $1 billion from the Bangladesh Central Bank alone, with the Federal Reserve Bank in New York processing $101 million.

## Requirement for Swift CSP

In response to the evolving threat landscape, Swift introduced the Customer Security Programme (CSP) in 2017, a framework designed to enhance its customers' cybersecurity. This first iteration of the CSP comprised 16 mandatory controls and 11 advisory controls, which were optional but all designed to promote better security posture.

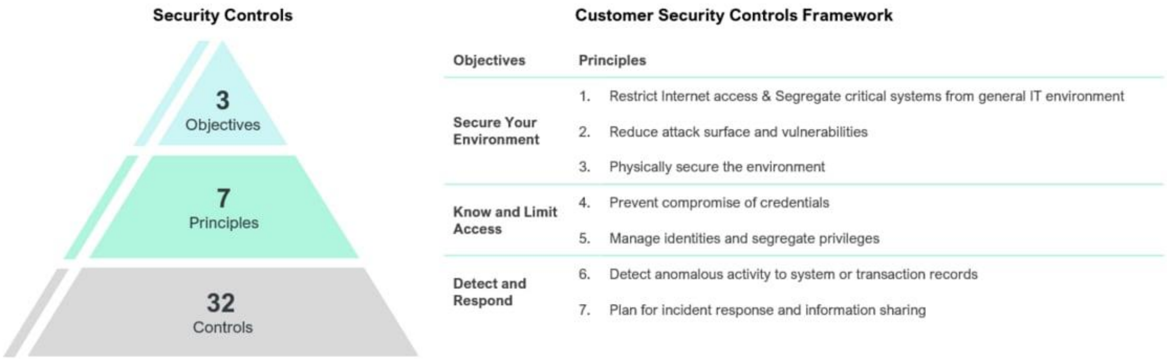
The CSP sets out controls that financial institutions must adhere to, to secure their Swift-related operations. Swift customers are always responsible for securing their own environments, but the CSP sets out a list of obligatory requirements to ensure the customer can continue to operate with Swift.

Compliance with CSP helps protect organisations from potential cyber threats and fosters trust and confidence among partners and customers. AMR CyberSecurity employs qualified, independent Swift Customer Security Programme (CSP) assessors, providing assurance for organisations seeking to comply with the Swift CSP.

## Overview of Swift CSCF

At the core of the CSP lies the Swift Customer Security Controls Framework (CSCF). This framework comprises mandatory and advisory security controls (22 mandatory and 8 advisory controls within the 2024 version), each addressing a specific aspect of cybersecurity.

The CSCF is split into 3 objectives, 7 principles and 32 controls.



Customer Security Controls Framework

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

Source: Swift.com

The framework covers various domains, including user access management, malware prevention and incident response, for example.

CSP guidelines include several reference architectures that relate to how the CSCF controls apply to your environment, and which controls are applicable depending on how you connect to the Swift network, how you limit the scope of processing within your environment to a secure environment, and where you use compliant third parties to process transactions on your behalf.

Swift issues an updated version of the CSCF every July. This updated version must then be used to support the organisation's attestation with the CSP through an independent assessment. The deadline for annual attestation is 31st December.

## Approach to Compliance

Achieving compliance with the CSP requires a proactive and holistic approach to cybersecurity. Organisations must implement the mandatory controls which are relevant to their Swift architecture and cultivate a cybersecurity culture across all levels.

This involves continuous risk assessment, vulnerability management and incident response planning. By implementing a strength-in-depth approach, organisations can effectively mitigate potential risks and respond promptly to emerging threats.

## Our Methodology to Assist Customers in Meeting the CSCF

As a dedicated cybersecurity consultancy and Swift CSP assessor company, we are committed to supporting our client's journey towards Swift CSP compliance.

Our methodology encompasses a tailored approach, beginning with a thorough assessment of the organisation's current cybersecurity posture.

We collaborate closely with our clients to develop and implement a roadmap that aligns with CSCF requirements. This roadmap includes identifying gaps, implementing necessary controls, employee training and education, and continuous monitoring to ensure ongoing compliance and security enhancement.

## Mapping CSCF Controls to Existing Frameworks

To facilitate a seamless integration of the CSP into existing cybersecurity practices, we offer a comprehensive mapping of CSCF controls to widely recognised frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the ISO 27001 standard. This alignment not only streamlines compliance efforts but also reinforces the cybersecurity measures already in place, maximising the value of cybersecurity investments.

## Conclusion

The Swift Customer Security Programme (CSP) is a critical initiative in safeguarding the integrity and security of the global financial ecosystem.

With cyber threats evolving at an unprecedented pace, organisations must proactively adopt measures that protect their customers, operations, data, and reputation.

By partnering with us - a reputable cybersecurity consultancy - and Swift CSP, organisations can navigate the complexities of CSP compliance, enhance their cybersecurity posture, and contribute to a safer financial environment for all stakeholders involved.

Together, we can build a more resilient and secure future for the financial industry.

## How We Can Help

It can be daunting to navigate the complexities of the Swift Customer Security Programme and its associated Customer Security Controls Framework.

At AMR CyberSecurity, we specialise in providing tailored cybersecurity consultancy services to ensure your organisation meets and exceeds Swift's stringent security requirements. Our expert team brings extensive experience in financial industry security, offering a comprehensive suite of services designed to enhance your compliance posture, mitigate risks and safeguard your operations.

## Supporting Services

1. **CSCF Pre-Assessment and Gap Analysis**
   - Conduct a detailed assessment of your current security posture against the CSCF controls.
   - Identify gaps and provide actionable recommendations to achieve full compliance.
2. **Control Implementation Support**
   - Assist with the implementation of security controls required by the CSCF.
   - Provide technical support and guidance to ensure controls are effectively integrated into your existing infrastructure.
3. **Security Policy and Procedure Development**

  - Develop and update security policies and procedures in line with CSCF requirements.
  - Ensure documentation meets regulatory standards and is easily understandable by your staff.

4. **Vulnerability Assessment and Penetration Testing**
    - Perform regular vulnerability assessments and penetration tests to identify and mitigate security weaknesses.
    - Provide detailed reports and remediation guidance.
5. **Incident Response Planning and Testing**
    - Develop and test incident response plans tailored to your organisation's specific needs.
    - Conduct tabletop exercises and simulations to ensure readiness for potential security incidents.
6. **Formal Assessment**
    - Carrv out final CSP external assessment

## Why AMR CyberSecurity?

By leveraging our expertise and comprehensive suite of services, AMR CyberSecurity will help you achieve robust security and compliance with the Swift Customer Security Controls Framework, allowing you to focus on your core business operations confidently.

Our staff includes Swift Certified Assessors.

Swift | **Provider**
Customer Security
Programme Assessment | 2025