SWIFT
„Customer Security Programme" CSP
Get Ready to be Prepared

Das SWIFT Customer Security Programme

In the last years the number of serious breaches in the banking industry through cyber-attacks has increased dramatically. Though every bank and every company is responsible for their own protection, SWIFT decided to take action and unite the industry in the fight against cyber crime by introducing the SWIFT „Customer Security Programme" (CSP).

SWIFT, the Society for Worldwide Interbank Financial Telecommunication, provides a global communication network that offers 24/7 secure international exchange of payment instructions and messages between all of its users.[1] SWIFT processes around 27,45 Mio. messages per day and has more than 11.000 users worldwide.[2]
The network itself has never been breached, but due to its role and importance in the financial industry the security within the network is critical to the industry.
As part of the „Customer Security Programme", which has been launched in 2016 SWIFT has introduced a set of cyber-security standards all of its users have to be compliant with.
This aims to reinforce the security of the financial industry and protect SWIFT users against cyber fraud.

Since the end of March 2017 the official Customer Security Controls Framework is accessible for all users of the SWIFT network. The framework explains all necessary security controls included in the CSP.

The security controls are based upon the three overarching framework objectives "Secure your Environment", „Know and Limit Access" and „Detect & Respond", and eight core principles. In total, 27 security controls are explained in the Customer Security Controls Framework, 16 of which are mandatory and 11 advisory.

All SWIFT users with a live 8-character BIC are required to provide a self-attestation against the mandatory controls by the end of 2017, irrespective of whether connecting directly or through a service provider. In the future this self-attestation has to be resubmitted at least on an annual basis or within a month when major changes occur.

The self-attestation status of each users has to be submitted into the KYC Registry Security Attestation Application[3] by December 31st 2017.
Every user has the authority over their

Key Facts and Dates

- Mandatory Self-attestation for all users of the SWIFT network
- 27 Security control (16 mandatory, 11 advisory)
- First self-attestation against mandatory controls until December 31st 2017, which has to be resumitted at least annually
- Submission of the self-attestation to the KYC Registry Security Attestation Application

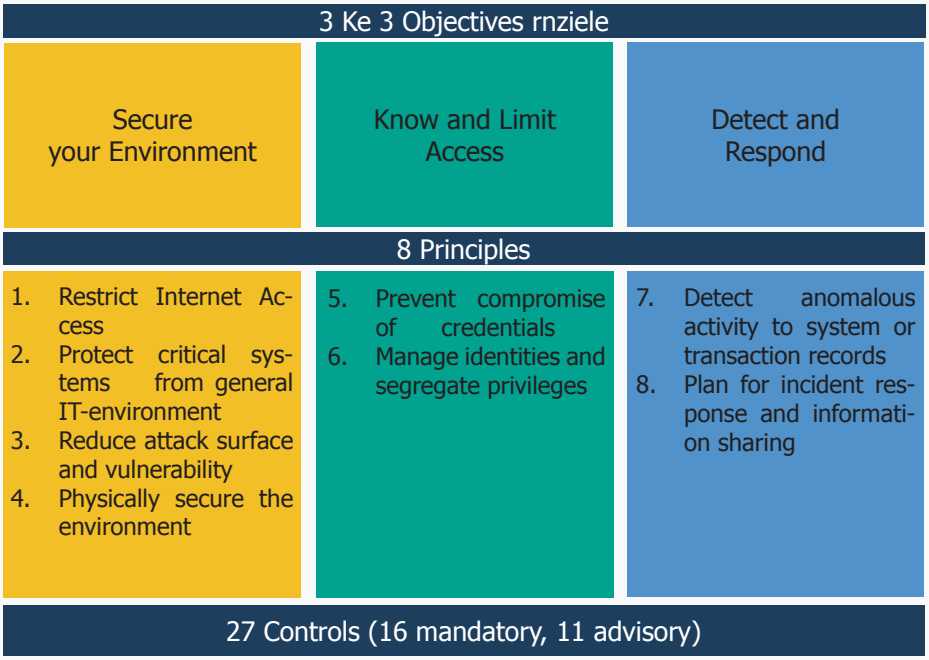
[1] Cf. Business Dictionary (URL) http://www.businessdictionary.com/definition/SWIFT.html
[2] Cf. SWIFT (URL) https://www.swift.com/about-us/swift-fin-traffic-figures#topic-tabs-menu

compliance status and will be able to grant other users access to their self-attestation status. But as of now every user can deny communicating with a user in the SWIFT network, who has a non-compliant or non-published status.

This increases transparency and security by enabling all users to apply risk-based decision-making to assess the counterparts with whom they wish to conduct business.

As of January 2018 SWIFT reserves the right to report all users that have not submitted a self-attestation to local supervisors. SWIFT also reserves the right to report users that have not self-attested compliance with all mandatory security controls (or that are connect through a non-compliant service provider) as of January 2019.

The SWIFT Customer Security Controls Framework (SWIFT CSC Framework)



Source: adapted from SWIFT

What Be FIS AG can do for you

The Be FIS AG can provide you with a broad range of Services regarding the „Customer Security Programme“:

- Review and analyze your current internal and external security infrastructure and existing security controls
- Perform a self-inspection in order to review the compliance status against the CSP controls and principles and to define any possible gaps in the security system that need to be addressed immediately
- Develop a SWIFT Compliance Report
- Implement all mandatory controls of the SWIFT Customer Security Controls Framework
- Implement advisory controls of the SWIFT Customer Security Controls Framework
- Develop and implement additional controls for further security and future compliance with the SWIFT Customer Security Controls Framework
- Support and train your team in all problems regarding SWIFT Compliance
- Support and implement all requirements after a SWIFT assessment for additional assurance
  Update your security infrastructure each year according the current SWIFT Customer Security Controls Framework

Be FIS AG is a worldwide established expert for SWIFT and its peripheral systems and supports your company in the implementation of all requirements of the „Customer Security Programme“ and the further development of your safety standards and controls.

Be SHAPING THE FUTURE

[3] tool designed for users to submit their self-attestation data which confirms their organisation's level of compliance with SWIFT's customer security controls.

Facts about Be FIS AG

- Specialist in the area of Payment, SWIFT and Info Management
- Consulting, IT-Services and Software
- Reliable partner for its clients since 1998
- Located in Germany
- Member of Be Group
- Comprehensive Know-how and long-term project experience in the area SWIFT
- International global players as clients
- Integrated consultancy approach

CONTACT

Be Shaping the Future -
Financial Industry Solutions AG
Fruehlingstraße 2
D-84034 Landshut
Tel: +49 (0) 871 27 66-0
information@rl-ag.com
www.be-stf.de