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

The 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 42,1 Mio. messages per day and has more than 11.000 participants 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.

To improve the security of global payments, SWIFT established the Customer Security Programme (CSP) in 2016, which requires SWIFT participants to implement security controls defined by SWIFT and provide an attestation on the level of compliance at the end of each calendar year.

All companies that participate in SWIFTNet for payment processing (i.e., have their own connected SWIFT BIC) must comply with the mandatory security controls of the SWIFT Customer Security Programme. These controls are documented in the SWIFT Customer Security Controls Framework (CSCF), which is updated at least annually. Each year, new controls are being introduced and advisory controls from the previous year are upgraded to mandatory ones on a regular basis.

These security controls are based on the three overarching framework objectives „Secure your Envi-

Data and Facts

- Mandatory submission of a attestation for all participants of the SWIFT network
- 31 security controls (22 mandatory, 9 advisory)
- Yearly submission of attestation based on the annually published and adjusted SWIFT CSCF
- From 2021, an Independent Assessment is necessary for the submission of the attestation
- Submission of the attestation via SWIFT KYC SA

[1] cf. Gabler Wirtschaftslexikon (URL) http://wirtschaftslexikon.gabler.de/Definition/swift.html
[2] cf. SWIFT (URL) https://www.swift.com/about-us/swift-fin-traffic-figures#topic-tabs-menu

Legal Disclaimer: All trademarks and trade names appearing in this document are fully subject to the provisions of the respective valid trademark laws and the rights of the registered owners.
For further information, please contact information@be-stf.de. All rights reserved.
© Be Shaping the Future - Financial Industry Solutions AG 2021

ronment", „Know and Limit Access" and „Detect & Respond", and eight security principles. A total of 31 security controls are listed in the Customer Security Controls Framework (CSCF), at most 22 of which are mandatory and, 9 advisory, depending on the architecture type.

Each SWIFT member must submit an annual attestation to the KYC Security Attestation Application (KYC-SA). From 2021, all SWIFT users are obligated to carry out an independent assessment when self-attesting. These can be done through either an internal or an external assessment, following the Independent Assessment Framework (IAF).

In addition to the IAF, SWIFT also reserves the right to mandate that an external assessment be undertaken.

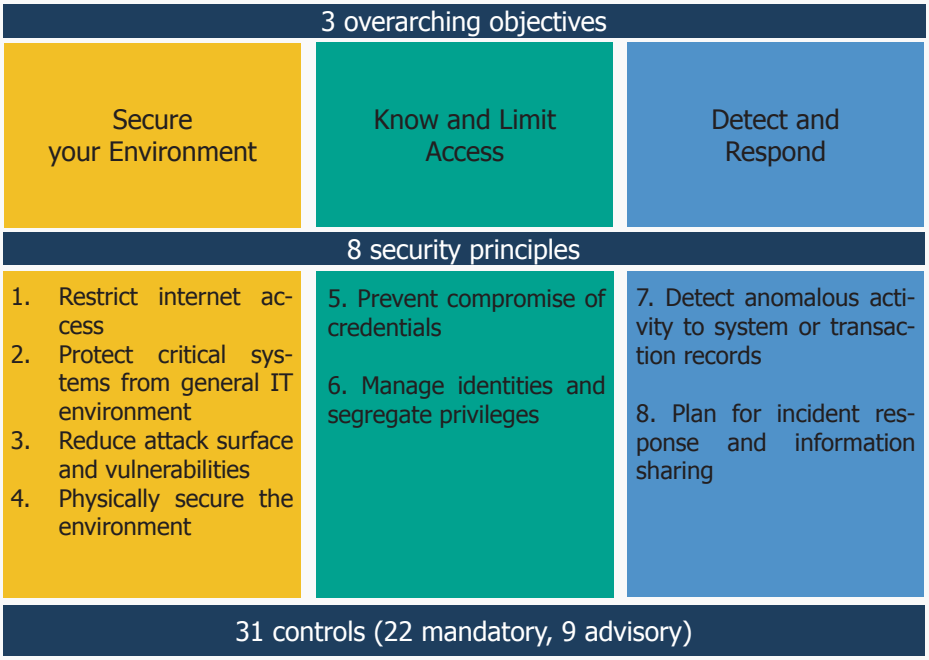
[3] Platform developed for users to submit their security attestation confirming the company's compliane status to SWIFT Customer Security Controls.

Be AG Facts

- 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 Soltutions AG
Frühlingstraße 2
D-84034 Landshut
Tel: +49 (0) 871 27 66-0
information@be-stf.de
www.be-stf.de

Customer Security Controls Framework (SWIFT CSCF)



Source: adapted from swift.de

What Be AG can do for you

The BE 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
- Develop feasibility studies
- Implement all mandatory controls of the SWIFT CSCF
- Implement advisory controls of the SWIFT CSCF
- Develop and implement additional controls for further security and future compliance with the SWIFT CSCF
- Support and train your team in all problems regarding SWIFT and the SWIFT Customer Security Programme
- Support and implement all requirements after an Independent Assessment
- Update your security infrastructure each year according the current SWIFT CSCF

BE 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

SWIFT Customer Security Programme

Legal Disclaimer: All trademarks and trade names appearing in this document are fully subject to the provisions of the respective valid trademark laws and the rights of the registered owners.
For further information, please contact information@be-stf.de. All rights reserved.

© Be Shaping the Future - Financial Industry Solutions AG 2021