TÜV TRUST IT
TÜV AUSTRIA Group

Security and value of information

New requirements for SWIFT users: The SWIFT Assessment

In the environment of large companies and financial systems, the security of IT infrastructures and related processes plays a particularly important role – especially due to the ever-increasing complexity of cyberattacks in this area. SWIFT users should note that while SWIFTNet enables secure payment transactions, it does not guarantee the security of the local environment of connected companies.

This is where the „Customer Security Programme“ (CSP) introduced by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) takes effect, which contains a series of security controls. In addition to this, obligatory and recommended controls are described in the SWIFT Customer Security Controls Framework (CSCF), so that SWIFT users can have the ability to easily follow all requirements to secure their SWIFT infrastructure and to defend against cyber-attacks.

Take precautions in time

So far, the concrete implementation of these requirements has been checked in the form of self-assessments and only had to be confirmed to SWIFT.

CSCF update process

The CSCF has been developed steadily since its introduction in 2018, with new recommended advisory controls being regularly added in line with the threat situation and previously introduced advisory controls being upgraded to mandatory controls.

With this approach, the SWIFT organisation strives for a continuous improvement of SWIFT infrastructures. The focus lies in particular on the following objectives:

1. Secure your environment
2. Know and limit access
3. Detect and respond

New from 2021:

SWIFT‘s request for an independent assessment on compliance with the specified controls.

Our recommendation:

Prepare for the new requirements now and have your compliance with the controls checked by an independent CSCF assessment.

Our service

TÜV TRUST IT offers a range of services for this purpose, to support you in the best possible way in realising the new requirements:

1. Realising the SWIFT CSP

Together with you, we analyse all specified security controls and support you in realising them in line with requirements. Within this framework following offer is available to you:

- Conduct a scoping workshop for the validation of the the SWIFT scope and the architecture type derived from it
- Comprehensive allocation of security measures from the information security management system (ISMS), if available
- Conducting workshops (typ. ½ day) on following topics:
  - Determination of the degree of compliance with SWIFT security controls at the target and implementation level (operationalisation of the requirements)
  - Derivation of concrete measures to achieve compliance with the SWIFT CSP at the target and implementation level

The experts of TÜV TRUST IT will be happy to support you as a SWIFT user by providing regular monitoring, e.g. in the form of Jour Fixe appointments incl. accompanying reporting.

TÜV TRUST IT
TÜV AUSTRIA Group

Security and value of information

2. SWIFT assessment

The staff of TÜV TRUST IT bring many years of confirmed expertise in the field of cyber security to our service and will be happy to assist you as a SWIFT customer with the SWIFT Customer Security Programme and the following topics:

- Conducting the SWIFT-compliant independent CSFC evaluations/assessments for SWIFT architectures A1, A2, A3, A4 and B
- Analysis of the existing infrastructure and security solutions
- Assessment of your control objectives and concrete recommendations regarding their optimisation
- Realisation of measures through technical solutions, products and consulting services

Recommendation: Take the opportunity now, using the SWIFT assessment to think about a holistic solution for your cybersecurity for your company - for more security in your company!

3. Certification of compliance on the basis of the SWIFT Independent Assessment Framework (IAF)

SWIFT users must annually certify their compliance with the mandatory controls relevant for the respective architecture in the form of a „self-attestation". Compliance must be verified as part of an assessment, which from 2021/2022 must be carried out by an independent body. In the usual community standard assessment, this can either be an internal control body such as the internal audit, the risk or compliance manager, or a qualified external service provider such as TÜV TRUST IT.

On the basis of the SWIFT Customer Security Framework we first assess your SWIFT infrastructure. An assessment based on the results then shows whether compliance with SWIFT requirements can be verified.

Your Benefits

- Fulfilment of the regulatory requirements for independent SWIFT assessment
- Building up know-how in your organisation
- Protection of internal ressources

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Phone: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Phone: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com