Crowe

SWIFT
Customer Security Programme

Audit / Tax / Advisory / Risk / IT

In 2021 all SWIFT users will be REQUIRED to undergo independent Customer Security Programme (CSP) assessment. In Crowe we can find an approach that suits best to your company and we are providing a service of an annual independent CSP review.

Banking information is some of the most important to keep safe. That's why recent high-profile cyber-attacks on customers using Society for Worldwide Interbank Financial Telecommunications (SWIFT) are so significant. After a series of high-profile attacks on the local environments of SWIFT customers, SWIFT responded by implementing the Customer Security Programme (CSP) to advise customers on how to mitigate the risk of fraud.

SWIFT's Customer Security Programme (CSP) helps financial institutions ensure their defences against cyberattacks are up to date and effective, to protect the integrity of the wider financial network.
From 2021, independent assessment will be an annual mandatory requirement for all SWIFT users.

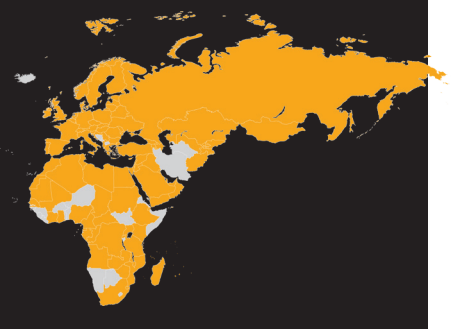
The CSP focusses on three mutually reinforcing areas. Customers will first need to protect and secure their local environment (you), which means securing your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber related fraud. Preventing and detecting fraud in your commercial relationships (your counterparts), and it means that companies do not operate in a vacuum and all SWIFT users are part of a broader ecosystem. Even with strong security measures in place, attackers are very sophisticated and you need to assume that you may be the target of cyber-attacks. That is why it is also vital to manage security risk in your interactions and relationships with counterparties.
And finally, continuously sharing information and preparing to defend against future cyber threats (your community). The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can be replicated elsewhere in the world.

SWIFT encourages its users to implement and monitor these customer security controls as part of a broader cyber security risk management program which should be regularly evaluated and adjusted, based on leading industry practices, and changes to the individual users security posture and infrastructure.

Contacts:

Crowe RS doo
Majke Jevrosime 23
11 000 Belgrade
T: +381 11 655 85 00
E: office@crowe.rs

Dejan Perić
Director / IT Advisory
T: +381 63 640 349
E: dejan.peric@crowe.rs



As of 2020, SWIFT has published an Independent Assessment Framework (IAF) to support its customers and their independent assessors in carrying out their responsibilities as part of the CSP. SWIFT member organizations must meet new compliance requirements, which includes an independent assessment, by 31 December 2021. SWIFT reports all cases of non-compliance along with instances where members have not attested at all to local regulators. In addition SWIFT will select a sample of attestations for validation each year to attest to meeting the controls, with results shared with counterparts and regulators.

Organisations must take a thoughtful and systematic approach, requiring collaboration across the three lines of defence, strong leadership and a diverse organised team and consulting experts as required in order to be successful.

In Crowe we can find an approach that suits best to your company and we are providing a service of an annual independent CSP review.

At Crowe, we understand the importance and complexities of cyber threats and information security in financial services. We connect the right people and knowledge to create teams that can keep clients ahead of market changes, through their insights, analysis and innovations.

Crowe has a number of services that can assist with the implementation of the SWIFT CSCF. These range from integrating the CSCF controls into your existing risk, governance and IT processes, to performing gap assessments, through to technical transformation of key systems, security, and network controls.

IN BRIEF

- SWIFT member organizations must meet new compliance requirements, which includes an independent assessment, by 31 December 2021.
- The new requirements impact SWIFT members as well as their ITOs and BPO
- Independent assessments require time, know-how and resources, and can be complex and challenging but using our experience and expertise we created a tailor made methodology based on WSHIFT CSCF and international security standards specific for this type of engagements.