

SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK

In July 2019 SWIFT released an updated version (v2020) of the Customer Security Controls Framework (CSCF) as part of the Customer Security Programme (CSP). We expect a new version being released in July 2020. The intention with releasing new versions is to evolve the framework to address new and arising threats, incorporate new advances in cybersecurity and to respond to feedback from the SWIFT community.

New and changing advisory requirements

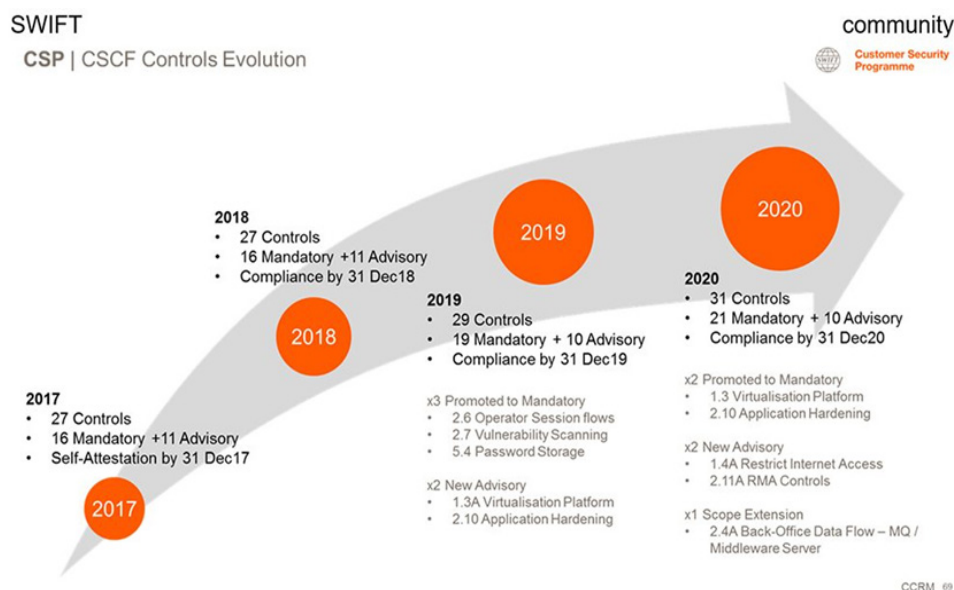
The CSCF v2020 introduced 2 new advisory requirements, promoted 2 requirements from advisory to mandatory and included one scope extension. The next version will likely follow the trend, described by SWIFT in the graphic below from the Customer Security Programme documentation, by introducing new controls and promoting selected controls from advisory to mandatory.

Independent assessment

With the release of CSCF v2020 SWIFT also introduced the independent assessment requirement for compliance attestation as opposed to the previous process where organization could attest their compliance without an independent assessor.

The new requirement details that compliance attestations need to include either:

- Internal assessment carried out by the company's second- or third- line of defence such as the users' internal compliance, internal risk of internal audit departments (independent from the first line of defence function submitting the attestation); or
- External assessment carried out by an independent external organisation with cyber security assessment experience and individual assessors who have relevant security industry certification.



Source: swift.com

Compliance with CSCF

It is mandatory for organizations using SWIFT's secure messaging services to comply with the CSCF and as with any other security standard or control framework, it is a journey.

No matter where you are on your journey, we at Seadot Cybersecurity offer our help with security and compliance challenges that arise on the path.

So, if you are in need of assistance in your SWIFT compliance programme, with for example scope adjustments, risk assessments, adjustments of controls or implementing new technology or processes controls, feel free to contact us for a discussion. We can also support you with other services in relation to CSCF v2020 or if you need assistance with a gap analysis related to new versions of the framework

Seadot Cybersecurity offers

Regulatory compliance is everywhere. Seadot Cybersecurity have extensive experience in regulations for instance for the financial market and we offer organizations in the financial industry our expertise. Compliance and security are complex and require a deep understanding of the ever changing technology and threat landscape as well as business and information risks. Through our experienced consultants we work together with the industry throughout the Nordics to implement efficient and effective ICT and security risk management.

Are you responsible for compliance, risk management or cyber security? Then reach out to Seadot Cybersecurity for an initial discussion on your challenges.