SWIFT Independent Assessment

Remain a trusted member of the network.

As part of its continuing Customer Security Program (CSP) to improve the cybersecurity of its members, SWIFT is making changes to its compliance requirements in 2021. From July 2021, self-attestation will no longer be sufficient to demonstrate compliance with the Customer Security Controls Framework (CSCF). All SWIFT members must undergo an independent assessment to confirm they meet all the requirements.

The CSP was introduced in 2016 following a series of successful attacks carried out over the SWIFT network. In one of the most prominent breaches, attackers made US$101 million in fraudulent transactions through a Bangladeshi bank. Several other banks and financial services organisations around the world were affected.

The SWIFT environment was not compromised in any of these attacks. Attackers bypassed local security measures at the member institutions.

CSP is designed to help prevent future attacks by setting minimum cybersecurity standards for all members of the SWIFT community.

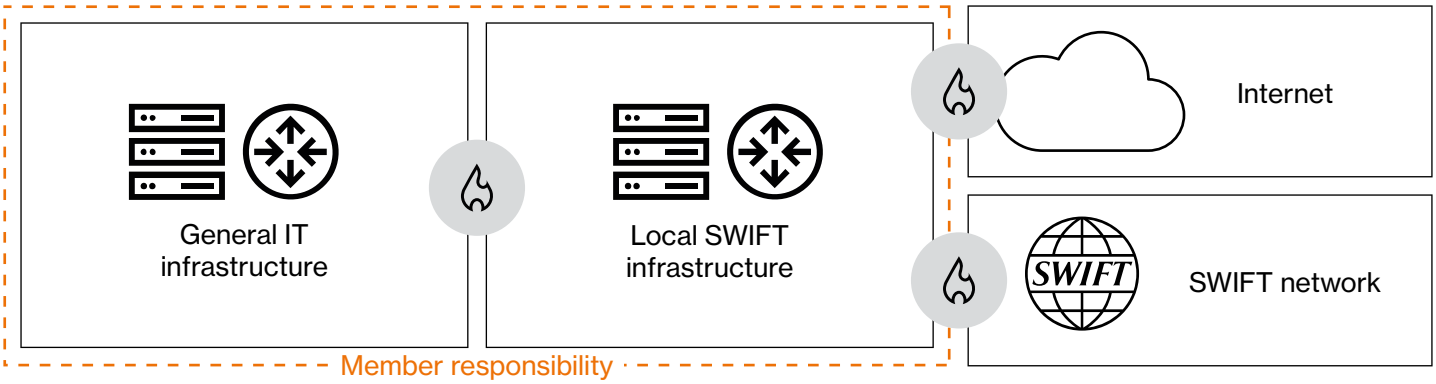
The CSCF provides security guidelines and audit frameworks to help organisations meet and show compliance with the CSP.

From 2021, self-attestation by the team managing SWIFT within the organisation is no longer acceptable. The CSCF assessment can be done internally – but it must be performed by a second- or third-line not directly connected to the company's SWIFT infrastructure. Organisations will need to provide sufficient documentation and evidence to substantiate their assessment and prove the independence of the team carrying out the attestation.

Alternatively, companies can use an approved third-party, like Verizon, to carry out the assessment and provide the attestation report. SWIFT publishes a Directory of Cyber Security Service Providers listing qualified third parties on its website.

verizon

SWIFT CSCF scope



Who, what and when

All SWIFT members must provide attestation of compliance with the mandatory security controls, regardless of whether they connect to SWIFT directly or indirectly.

Compliance with CSCF must be shown for each bank identifier code (BIC) that the organisation uses.

The CSCF defines the scope of what infrastructure and processes are covered. As of February 2021, the framework consists of 31 controls – see next page for details. The number and specifics of these security controls is subject to change to keep pace with the evolving threat landscape.

Organisations that aren't able to demonstrate independent attestation by 31 December 2021 face significant obstacles to future SWIFT payments and business dealings.

A list of non-compliant companies will be published on the SWIFT website and the relevant local monetary authorities, central banks and financial regulatory agencies notified. SWIFT will also notify counterparties to the transaction if one of them is not compliant with the CSCF.

More than compliance

It's been said that all banks have to sell is trust. The CSCF is designed to improve security across the more than 11,000 institutions that make up the SWIFT network. This will help the network remain a safe and reliable place to do business.

Compliance should be more than a 'tick-box' exercise. Verizon takes a holistic approach to security and compliance. This approach can help reduce the cost and management burden of meeting regulations.

To reduce the burden on members, SWIFT has published mappings of CSCF to Payment Card Industry (PCI) Data Security Standard (DSS), ISO 27002 and NIST standards.

As a leading cybersecurity practitioner, Verizon can also help organisations to improve the maturity and robustness of their security controls. This is vital to improving security and maintaining compliance between assessments.

A pragmatic approach

Our pragmatic approach to CSCF attestation is based on six steps:

1 Define scope

We'll ask you to complete the SWIFT welcome package to clearly define the scope of compliance – whether it's functional, technical or organisational.

2 Preliminary review

We'll then perform a preliminary check of all the information provided before beginning our assessment.

3 Remote review

We'll perform a remote review based on the documentation and evidence provided.

4 On-site assessment

Followed by on-site assessment interviews based on a planned schedule, and collect further evidence on-site.

5 Second review

We'll then perform our second review, on site or remotely, to ensure compliance gaps were successfully remediated with priority given to mandatory controls.

6 Assessment report

Finally, we provide you with an assessment report via the CSCF Assessment Tool, independent assessment letter and executive presentation.

Independent attestation

Successful independent attestation of compliance with CSCF security controls.

SWIFT cybersecurity frameworks

SWIFT's CSP and CSCF are based around three key objectives and eight core security principles. The CSCF lists the specific security controls needed and accompanying guidelines for demonstrating compliance. This has grown from a total of 27 controls in 2017 to 31, 21 mandatory and 10 advisory, in 2021.

Customer Security Programme (CSP)		Customer Security Controls Framework (CSCF)		
3 objectives	8 principles	31 controls: 21 mandatory and 10 recommended		
Secure your environment	Protect critical systems from the general IT environment	**1**	1.1	SWIFT environment protection
			1.2	Operating system privileged account control
			1.3	Virtualisation platform protection
	Restrict internet access		1.4	Restrict internet access
	Reduce attack surface and vulnerabilities	**2**	2.1	Internal data flow security
			2.2	Security updates
			2.3	System hardening
			2.4	Back office data flow security
			2.5	External transmission data protection
			2.6	Operator session confidentiality and integrity
			2.7	Vulnerability scanning
			2.8	Critical activity outsourcing
			2.9	Transaction business controls
			2.10	Application hardening
			2.11	RMA business controls
	Physically secure the environment	**3**	3.1	Physical security
Know and limit access	Prevent compromise of credentials	**4**	4.1	Password policy
			4.2	Multi-factor authentication
	Manage identities and segregate privileges	**5**	5.1	Logical access control
			5.2	Token management
			5.3	Personnel vetting process
			5.4	Physical and logical password storage
Detect and respond	Detect anomalous activity to systems or transaction records	**6**	6.1	Malware protection
			6.2	Software integrity
			6.3	Database integrity
			6.4	Logging and monitoring
			6.5	Intrusion detection
	Plan for incident response and information sharing	**7**	7.1	Cyber incident response planning
			7.2	Security training and awareness
			7.3	Penetration testing
			7.4	Scenario risk assessment

Mandatory | Made mandatory in 2020 | Recommended | Added as advisory in 2020

Look no further

We're no stranger to helping companies achieve, demonstrate and maintain compliance. Our expertise means we're perfectly positioned to help you with your SWIFT CSCF attestation.

Less burden for you

SWIFT by name, swift by nature. Our experience performing assessments and established processes mean that we can carry out your CSCF attestation more quickly and efficiently. As well as reducing the burden on the internal team – remember it has to be from another part of the organisation – we can reduce the impact on business processes.

More predictable cost

Our proven approach means that we can identify and help you address any potential issues quickly. This increases the likelihood of successful attestation by the deadline. And unlike using an internal team that's not experienced in performing such audits, we can give you an accurate scope upfront. Because of this, we're able to set a price and stick to it.

Greater peace of mind

We wrote the book on cybersecurity. Actually we write several of the industry's most highly regarded publications each year.

Each of our assessors are highly trained with significant practical experience. Our team holds numerous certifications, from technical – such as CISSP, CISM, CISA, and CRISC – to industry regulation – such as PCI DSS QSA, PA-QSA and P2PE.

When you choose Verizon, you can rest assured that you're putting your CSCF attestation in safe hands.

Verizon has been positioned as a Leader in the Gartner Magic Quadrant Managed Security Services, Worldwide for seven successive years.

Related services

Verizon has been recognised as a leader in cybersecurity and is a leading provider of services to the financial services industry.

PCI DSS Assessment

We have over 10 years of experience in performing security compliance assessments. This includes having one of the largest teams of PCI DSS qualified security assessors (QSAs) in the world. Many leading banks, retailers and other organisations trust us to carry out their assessments year after year.

Our PCI DSS experts can help you assess, manage and implement a plan to help your business maintain compliance and cybersecurity resilience. This includes helping you identify gaps and how to address them.

Find out more

Security Program Assessment

Get an objective evaluation of your security program against your preferred industry security framework or regulatory requirement. We provide an objective and repeatable measure of your security program to help you move toward control maturity.

Find out more

Threat intelligence services

Learn the risks most relevant to your organization based on analysis of the surface, deep and dark webs. As a leading security provider with one of the largest global IP networks, our threat intelligence services give you unparalleled visibility and insight into the evolving threat landscape.

Find out more

Get started

Let us help you complete your CSCF attestation submission so you can focus on managing and growing your business.

Contact us >

verizon