A CYBER 1 Company

> > >

Swift CSP

Services

Swift CSP Services - what is it?

SWIFT has published a set of core security controls that every SWIFT customer must meet. These controls reflect good security practice and should apply to all systems and processes within the end-to-end transaction chain.

A formal introduction of the SWIFT Customer Security Controls standard was issued in April 2017.

The CSP standard covers detailed security controls (16 mandatory and 11 advisory) which support three overarching security objectives which address major areas of attention for cyber-security efforts. These three objectives are supported by eight principles:

Secure Your Environment
1. Restrict internet access
2. Protect critical systems from general IT environment
3. Reduce attack surface and vulnerabilities.
4. Physically secure the environment

Know and Limit Access
5. Prevent compromise of credentials
6. Manage identities and segregate privileges

Detect and Respond
7. Detect anomalous activity to system or transaction records
8. Plan for incident response and information sharing

Each security control is supported by recommended implementation details, a description of the IT components it relates to as well as suggested optional enhancements.

A CYBER 1 Company

Swift CSP

Services

Why do i need swift CSP Services?

SWIFT requires customers to provide self-attestation against the mandatory controls. The requirements will be immediately applicable to all users connected to SWIFT.

When do i need it?

As of April 2017 users can already begin to evaluate their compliance against the security controls and prepare for self-attestation as of July 2017 via the self-attestation folder in the KYC Registry. By 01 January 2018, all users MUST have submitted their self-attestation and users will be required to resubmit their attestation on an annual basis thereafter.

Customers may make their compliance status available to their counterparties (via a security attestation folder in the KYC Registry), providing transparency and allowing other users on the network to apply risk-based decision making regarding their counterparty relationships.