FINASTRA

Factsheet – Fusion Total Messaging

SWIFT CSP independent assessment services offered by Finastra

Helping to promote cybersecurity within the SWIFT user community

> ***"As CSP has evolved year-on-year, it has significantly raised the community's cybersecurity awareness and bolstered defenses. Evidence points to a dramatic fall-off in cyber attacks successfully targeting the back-office infrastructures of SWIFT-connected financial institutions....But it is rare that fraud just disappears."***

[Why you should be rethinking SWIFT CSP compliance]

Roy Belchamber, *Head of Product Management, NetGuardians, March 2022*

The number of cyber threats in the financial community continues to grow and evolve. Over the last few years, fraudulent activities have resulted in the disruption and misdirection of payment processing and payment fraud, ultimately resulting in financial and reputational damage.

As the world's largest provider of secure financial messaging services to banks and other financial institutions, SWIFT is an appealing target to cybercriminals. To help combat fraudulent activities, SWIFT now mandates that all financial institutions using SWIFT need to support their Customer Security Programme (CSP) attestations with an independent internal or external assessment on an annual basis. In addition, effective from July 2022, there is one very significant change: control 2.9 (transaction business controls) is mandatory. The objective of this control is to ensure banks monitor to know that transaction activity is within the expected bounds of normal business.

To ensure SWIFT members are compliant with these new mandates, Finastra now provides independent CSP assessment services.

What is the CSP?

SWIFT's Customer Security Programme (CSP) is a common set of security controls aimed at assisting users to secure their SWIFT environments. The SWIFT Customer Security Controls Framework (CSCF) consists of both mandatory and advisory security controls. These mandatory security controls establish a general security baseline and must be implemented by all users, including those that use a Service Bureau.

Advisory controls are based on sound security practice, and it is recommended that users adopt these controls where applicable.

The goal of CSP is to mitigate the risk of fraudulent activities through a set of controls; this includes the independent assessment requirement. The list of controls will be regularly reviewed by SWIFT based on the evolving cyber threat landscape.

The assessment can be performed through an independent external organization, such as Finastra, which has existing cybersecurity assessment experience and individual assessors who have relevant security industry certifications.

3x

Global losses from payment fraud has more than tripled since 2011.

$40 billion

Payment fraud is expected to continue increasing and projected to exceed $40 billion by 2027.

Global Payment Fraud Statistics, Trends & Forecasts, October 2020 - https://www.merchantsavvy.co.uk/payment-fraud-statistics

Finastra: Your trusted provider

Finastra stands ready with an experienced team in place with extensive knowledge in payments, cybersecurity, financial services regulatory compliance and technology risk management to provide your organization with a SWIFT CSP attestation report.

Finastra is listed on SWIFT's directory of independent CSP providers after demonstrating the required criteria:

- Cybersecurity services experience and credentials
- Strategic focus on cybersecurity services
- Good reputation and commitment to customers in the financial industry

As an independent assessor, Finastra has developed a CSP service for all SWIFT members and its Service Bureau customer.

Finastra's CSP service includes:

- Scope and architecture type assessment
- Project plan to achieve attestation
- Scope document detailing architecture model; relevant infrastructures and applications; message flows; users and in-scope assets
- Controls tracker – a detailed breakdown of compliance against each CSCF control requirement
- Attestation report – detailed findings against each SWIFT CSCF control, including supporting evidence, assessment, gap analysis and recommendations
- Remediation report, including remediation path
- Executive summary report
- Bi-monthly steering group follow up (optional)

Our CSP service is tailored as infrastructures, implementations, integrations and their complexities are unique to each customer.

Assessment scope

Finastra's assessment scope covers all mandatory controls and components of the SWIFT-related infrastructure, which include the following:

- Data exchange layer
- Local SWIFT infrastructure
  - Secure zone
  - Messaging interface
  - Communication interface
  - SWIFTNet Link (SNL)
  - Connector
  - SWIFT hardware security modules (HSMs)
  - Firewalls, routers and switches within or surrounding the SWIFT infrastructure
  - Graphical user interface (GUI)
  - Jump server
  - Virtualization platform
  - Dedicated operator PC
- Operators and their general purpose operator PCs

The assessment confirms the architecture type selected and encompasses all production, disaster recovery, and/or backup environments (as applicable) that house any of the above systems, operators or devices.

Why use Finastra as your independent assessor

- With proven SWIFT and industry expertise, SWIFT lists Finastra as a trusted independent CSP provider
- Finastra has the required cybersecurity assessment experience, with guaranteed oversight by Finastra's security industry certified experts
- Finastra's streamlined CSP processes check against SWIFT's CSCF controls
- Finastra provides transparency of findings for input to your KYC filings
- We offer a remediation path for items to be addressed
- Existing Service Bureau customers benefit from Finastra's insights in their environment, which speeds the process

To learn more about Finastra's CSP Assessment Services, please contact your Account Manager or Contact Us.

About Finastra

Finastra is building an open platform that accelerates collaboration and innovation in financial services, creating better experiences for people, businesses and communities. Supported by the broadest and deepest portfolio of financial services software, Finastra delivers this vitally important technology to financial institutions of all sizes across the globe, including 90 of the world's top 100 banks. Our open architecture approach brings together a number of partners and innovators. Together we are leading the way in which applications are written, deployed and consumed in financial services to evolve with the changing needs of customers. Learn more at **finastra.com**

Corporate Headquarters
4 Kingdom Street
Paddington
London W2 6BD
United Kingdom
T: +44 20 3320 5000

ID-19474 / 0422