Grant Thornton

An instinct for growth™

SWIFT assurance and security services

April 2019

SWIFT has a set of security standards that are mandatory for all SWIFT customers. As SWIFT registered partners, Grant Thornton has been supporting clients and the SWIFT community in assessing and implementing SWIFT security practices.

For this reason, we are uniquely positioned to help you achieve compliance with your SWIFT internal attestation, audit or third party inspection. Due to recent high profile thefts and cyber security breaches in multiple banks, the new security standard has been introduced to establish a baseline security requirement across the community. To ensure compliance, SWIFT requires all customers to submit their self-attestation status into SWIFT's online KYC Registry on an annual basis and annually thereafter. To foster transparency, customers can allow their counter-parties to view their self-attestation status.

Three differing assurance requirements depending on the type of SWIFT participant

Self attest: your own assessment:

- required for all SWIFT customers;
- a SWIFT participant asserts that they are compliant with the security requirements;
- demonstration of controls within operations teams;
- the positive assertion is provided by senior management;
- demonstration of effective and operating controls;
- clear remediation plans for control gaps; and
- effective reporting on control performance.

Self inspect: internal audit assessment:

- your internal audit reviews and asserts to the SWIFT self-assessment completed by your operations team;
- internal audit reviews and identifies control gaps around the 29 key control areas; and
- internal audit reports on adequacy of control design and operational effectiveness to management.

Third-party inspections:

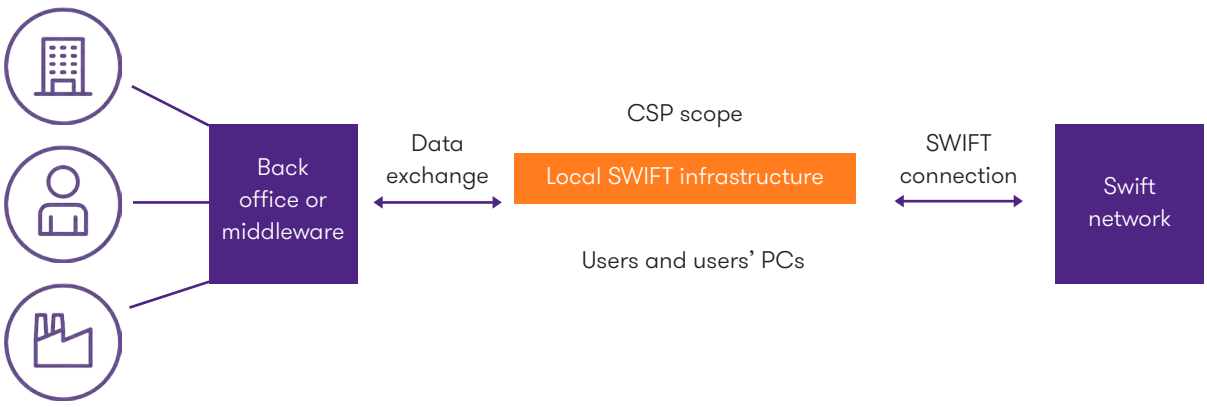
- required for a subset of SWIFT customers based on systemic risk and size;
- an external independent third party assesses the attestation and validates the customer's assertion; and
- independent control effectiveness reporting to senior management and SWIFT. This includes identification of common weaknesses that may pose systemic risk to the SWIFT network.

Other related SWIFT challenges

Malware and ransomware
Malware played a crucial part in the recent security breaches and theft incidents and SWIFT has published updates to its alliance application suite informing members of a growing threat from ransomware and malware. Our team has deep insights in this area and can support clients in managing this risk.

Payment chain and transaction security
The integration of messaging and settlement systems has resulted in fragmented transaction processing chains and applications managed by separate teams. This fractured view of end to end transaction integrity makes it difficult to implement security in depth. Our payment and messaging experts can support clients in managing this risk.

Scope of security controls



Scope of CSP security controls

The CSP scope and controls are applicable to the Data exchange layer, Local SWIFT infrastructure, User PCs and Users. The back office applications and SWIFT's owned network remain out of scope.

Mandatory Controls

Restrict Internet Access and Protect Critical Systems from General IT Environment:

- SWIFT Environment Protection
- Operating System Privileged Account Control

Reduce Attack Surface and Vulnerabilities:

- Internal Data Flow Security
- Security Updates
- System Hardening
- Operator Session Confidentiality and Integrity
- Vulnerability Scanning

Physically Secure the Environment:

- Physical Security

Prevent Compromise of Credentials:

- Password Policy
- Multi-factor Authentication

Manage Identities and Segregate Privileges:

- Logical Access Control
- Token Management
- Physical and Logical Password Storage

Detect Anomalous Activity to Systems or Transaction Records:

- Malware Protection
- Software Integrity
- Database Integrity
- Logging and Monitoring

Plan for Incident Response and Information Sharing:

- Cyber Incident Response Planning
- Security Training and Awareness

Advisory Controls

Restrict Internet Access and Protect Critical Systems from General IT Environment:

- Virtualisation Platform Protection

Reduce Attack Surface and Vulnerabilities:

- Back-office Data Flow Security
- External Transmission Data Protection
- Critical Activity Outsourcing
- Transaction Business Controls
- Application Hardening

Manage Identities and Segregate Privileges:

- Personnel Vetting Process

Detect Anomalous Activity to Systems or Transaction Records:

- Intrusion Detection

Plan for Incident Response and Information Sharing:

- Penetration Testing
- Scenario Risk Assessment

How can we help

Our payments team is comprised of banking, SWIFT, payment messaging and cyber security experts who form part of the **Grant Thornton's SWIFT Security Centre of Excellence**. Our SWIFT assurance services deliver full SWIFT security compliance assessment of SWIFT and interfacing applications, underlying infrastructure and operational processes to meet current requirements. Our teams can also design a target operating model to help embed the required controls, structures and processes into your organisation. As a SWIFT partner, our assurance, risk management and payments security services help our clients mitigate risk, hereby protecting operating profits, achieving compliance and increasing operating confidence. Grant Thornton complements SWIFT's own services and portfolio enabling our customers to make well informed SWIFT purchasing and implementation decisions. This differentiates our offering in a crowded marketplace.

For further information, please contact:

Christos Makedonas
Managing Director
Technology Risk Services
T +357 22600000
E Christos.Makedonas@cy.gt.com

Grant Thornton
An instinct for growth™

grantthornton.com.cy