Grant Thornton

An instinct for growth™

SWIFT assurance and security services

SWIFT has released a set of security standards that will be 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 by end of 2017 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:

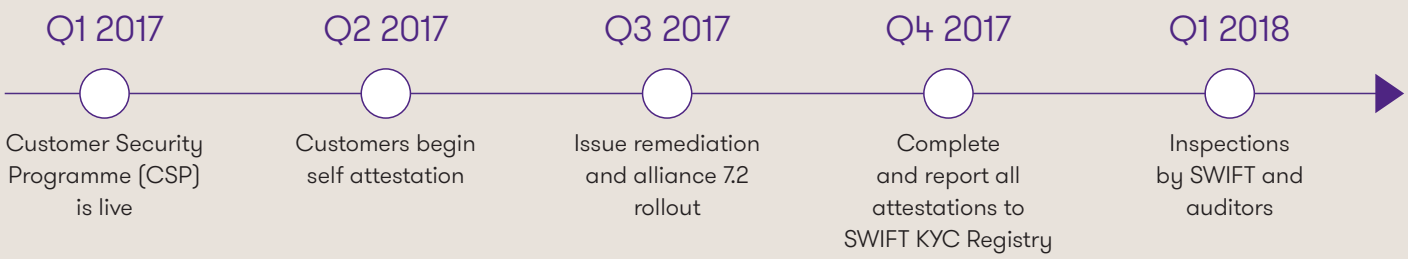
- your internal audit reviews and asserts to the SWIFT self-assessment completed by your operations team;
- internal audit reviews and identifies control gaps around the 27 key control areas; and
- internal audit reports on adequacy of control design and operational effectiveness to management.

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.

Key dates

These are initial key dates within the certification programme. The aim is for all participants to comply with CSP before 1 January 2018. SWIFT will be holding road shows to increase publicity and community engagement



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.

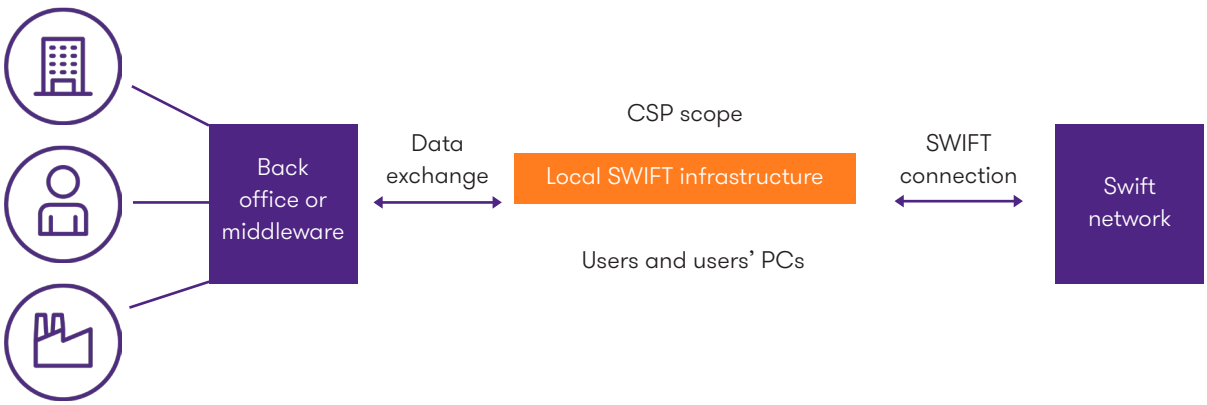
SWIFT mandatory software release

The next mandatory technology and software change for SWIFT 7.2 is planned for June 2017. This release is crucial as it underpins SWIFT's continuing efforts to provide a highly secure and efficient service. This upgrade requires detailed planning and all customers are required to implement it by September 2018.

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

- SWIFT environment segregation and operating system privileged account control;
- reduce attack surface and vulnerabilities: internal data flow security, security updates and system hardening;
- physically secure the environment;
- prevent compromise of credentials: password policy and multi-factor authentication;
- manage identities and segregate privileges: user account management and token management;
- detect anomalous activity to systems or transaction records: malware protection, software integrity, database integrity and logging and monitoring; and
- plan for incident response and information sharing: cyber incident response planning and security training and awareness.

Advisory controls

Reduce attack and surface and vulnerabilities:

- back office data flow security;
- external transmission data protection;
- user session integrity;
- vulnerability scanning; and
- critical activity outsourcing.

Manage identities and segregate privileges:

- personal vetting process; and
- physical and logical password storage.

Detect anomalous activity to systems or transaction records:

- intrusion detection.

Plan for incident response and information sharing:

- scenario risk assessment; and
- penetration testing.

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.

Contact

Please contact a member of our team below for further information and discussion.

Mike Harris
Partner, Cyber Security
T +353 (0)1 436 6503
E mike.harris@ie.gt.com

Rohan Singla
Associate Director, Cyber Security
T +353 (0)1 680 5804
E rohan.singla@ie.gt.com

Over 1,000 people operating from offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

www.grantthornton.ie

#GTcyber

Grant Thornton Ireland

Grant Thornton
An instinct for growth™

grantthornton.ie

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing.

© 2017 Grant Thornton Ireland. All rights reserved. Authorised by Chartered Accountants Ireland ("CAI") to carry on investment business. 'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.