SWIFT Customer Security Programme
The essentials

What is the SWIFT Customer Security Programme?

SWIFT Customer Security Programme (CSP)

The SWIFT CSP focuses on three mutually reinforcing areas. Protecting and securing your local environment (You), preventing and detecting fraud in your commercial relationships (Your counterparts) and continuously sharing information and preparing to defend against future cyber threats (Your community).

While all customers remain primarily responsible for protecting their own environments, SWIFT's CSP aims to support its community in the fight against cyber-attacks.

Why is it important?

In response to a number of cyber attacks and breaches throughout 2016, SWIFT has identified 16 mandatory and 11 optional security controls for all its 11,000 customers worldwide. All customers will be asked to attest to meeting the controls, with results shared with counterparts and regulators.

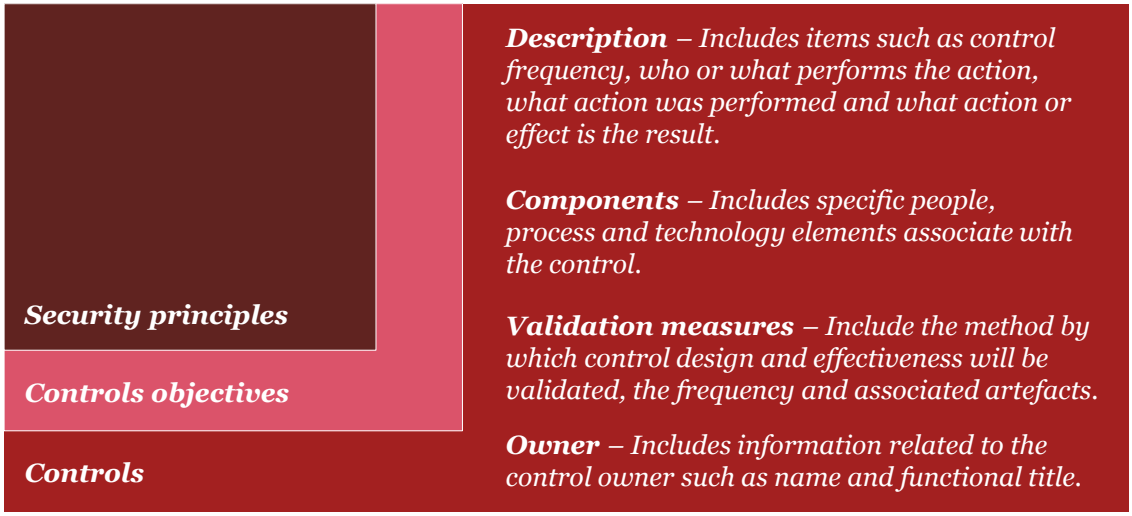
Impact

Impacts will vary depending on the maturity of the organisation, the design of the local SWIFT environment and the nature of existing controls. Many organisations will need to remediate both technical and process related gaps.

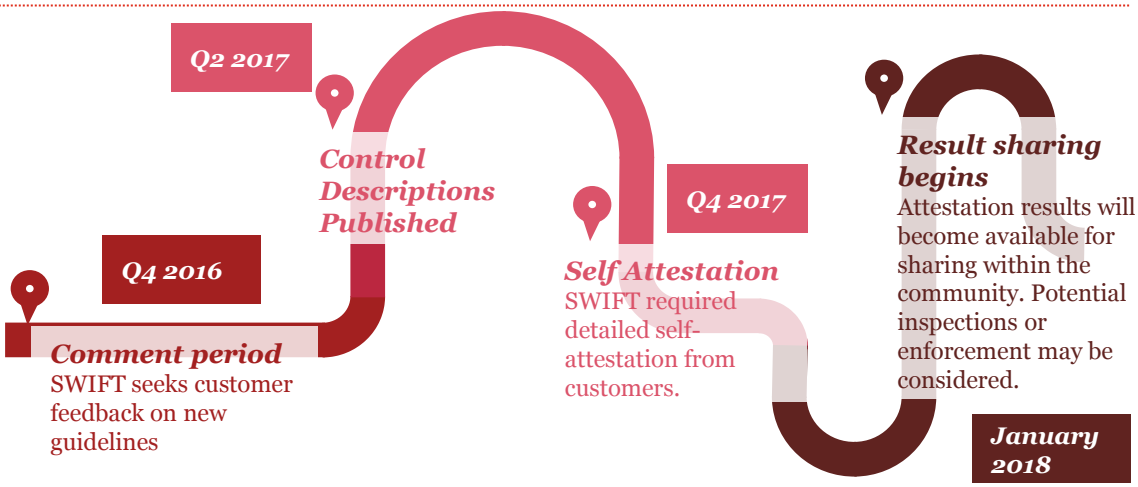
Success factors

To be successful, organisations must take a thoughtful and systematic approach, requiring collaboration across the three lines of defence, strong leadership and a diverse organised team.

Cyber security assurance framework



Timeline



SWIFT Customer Security Programme
PwC capabilities

How can PwC help?

Gap analysis — 1

Perform assessment to determine if current controls exist which satisfy SWIFT requirements.

Remediation — 2

Develop workstreams to address identified controls gaps via both technology and process changes.

Attestation — 3

Validation of successful compliance with the CSP controls and transition to on-going compliance team.

Additional services

Cyber security services:

- *Penetration testing*
- *Technical benchmarking*
- *Red-team testing*
- *Breach indicator assessments*

Performance assurance services:

- *Third Party Controls reporting under recognised standards (e.g. SOC2, ISAE)*
- *Trust analytics – Measuring levels of trust within your customer base*

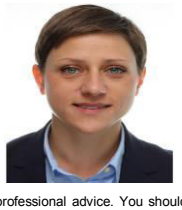
Why PwC?

Cohesive team who understand SWIFT	*PwC understands SWIFT like no other as we have been performing an annual review of SWIFT under the internationally recognised ISAE3000 standard for over 10 years.*
Proven performance on similar projects	*PwC have performed numerous SWIFT security assessments worldwide and as such, we have a proven approach and understanding of how to ensure the security of SWIFT infrastructure, while maintaining functionality.*
Technical expertise and knowledge base	*PwC is the only 'Big-4' firm with a professional Certified Cyber Security Consultancy certificate from the NCSC. PwC are unique in our ability to leverage threat intelligence to build and simulate realistic cyber attack scenarios.*
Adapting to your requirements	*PwC will formulate and tailor an approach that suits your immediate requirements and future ambitions. To achieve those PwC will provide pragmatic insights and balanced views on how to prioritise any associated actions.*

Gerwin Naber
Partner
M: +31 (0)651 507 575
E: gerwin.naber@pwc.com

Bram Van Tiel
Director
M: +31 (0)622 432 962
E: bram.van.tiel@pwc.com

Bas Rebel
Senior Director
M: +31 (0)645 874 974
E: bas.rebel@pwc.com



Olena Kernasovska
Senior Manager
M: +31 (0)630 975 092
E: o.kernasovska@pwc.com

SWIFT Customer Security Programme
Appendix (1/2)

SWIFT Customer security controls framework overview

This overview section establishes the set of mandatory and advisory security controls. Mandatory security controls build on existing guidance and establish a security baseline. Advisory controls are optional good practices that SWIFT recommends each user implement in their environment.

Objectives	Principles	Controls
Secure Your Environment	Restrict Internet Access and Protect Critical Systems from General IT Environment	***Mandatory*** **SWIFT Environment protection –** A segregated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments. Operating System Privileged Account Control – Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with least privilege access is used.
	Reduce Attack Surface and Vulnerabilities	***Mandatory*** **Internal data flow security** – Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT-related application-to-application and operator-to-application data flows. **Security updates** – All hardware and software inside the secure zone and on operator PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied. **System hardening** – Security hardening is conducted on all in-scope components. ***Advisory*** **Back-office data flow security** – Confidentiality, integrity, and mutual authentication mechanisms are implemented to protect data flows between back office (or middleware) applications and connecting SWIFT infrastructure components. **External transmission data protection** – Sensitive SWIFT-related data leaving the secure zone is encrypted. **Operator session confidentiality and integrity** – The confidentiality and integrity of interactive operator sessions connecting into the secure zone is safeguarded. **Vulnerability scanning** – Secure zone and operator PC systems are scanned for vulnerabilities using an up-to-date, reputable scanning tool. **Critical activity outsourcing** – Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation. **Transaction business controls** – Implement RMA controls and transaction detection, prevention and validation controls to restrict transaction activity to within the expected bounds or normal business.
	Physically Secure the Environment	***Mandatory*** **Physical security**– Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

SWIFT Customer Security Programme
Appendix (2/2)

Objectives	*Principles*	*Controls*
Know and Limit Access	Prevent Compromise of Credentials	***Mandatory*** **Password policy** – All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed log-in attempts. **Multi-factor authentication** – Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.
	Manage Identities and Segregate Privileges	***Mandatory*** **Logical access control** – Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties. **Token management** – Connected hardware authentication tokens are managed appropriately during issuance, revocation, use, and storage. ***Advisory*** **Physical and logical password storage** – Any recorded passwords for privileged accounts are stored in a protected physical or logical location, with access restricted on a need-to-know basis.
Detect and Respond	Detect Anomalous Activity to Systems or Transaction Records	***Mandatory*** **Malware protection** – Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems. **Software integrity** – A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications. **Database integrity** – A database integrity check is performed at regular intervals on databases that record SWIFT transactions. **Logging and monitoring** – Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs. ***Advisory*** **Intrusion detection** – Intrusion detection is implemented to detect unauthorised network access and anomalous activity.
	Plan for Incident Response and Information Sharing	***Mandatory*** **Cyber incident response planning** – The organisation has a defined and tested cyber incident response plan. **Security training and awareness** – Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access. ***Advisory*** **Penetration testing** – Application, host, and network penetration testing is conducted within the secure zone and on operator PCs. **Scenario risk assessment** – Scenario-driven risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organisation's security programme.