KPMG

SWIFT - Customer Security Programme (CSP) and Controls

February 2017

Bermuda

SWIFT Customer Security Program - Background

The last year has seen multiple SWIFT related hacks at banks:

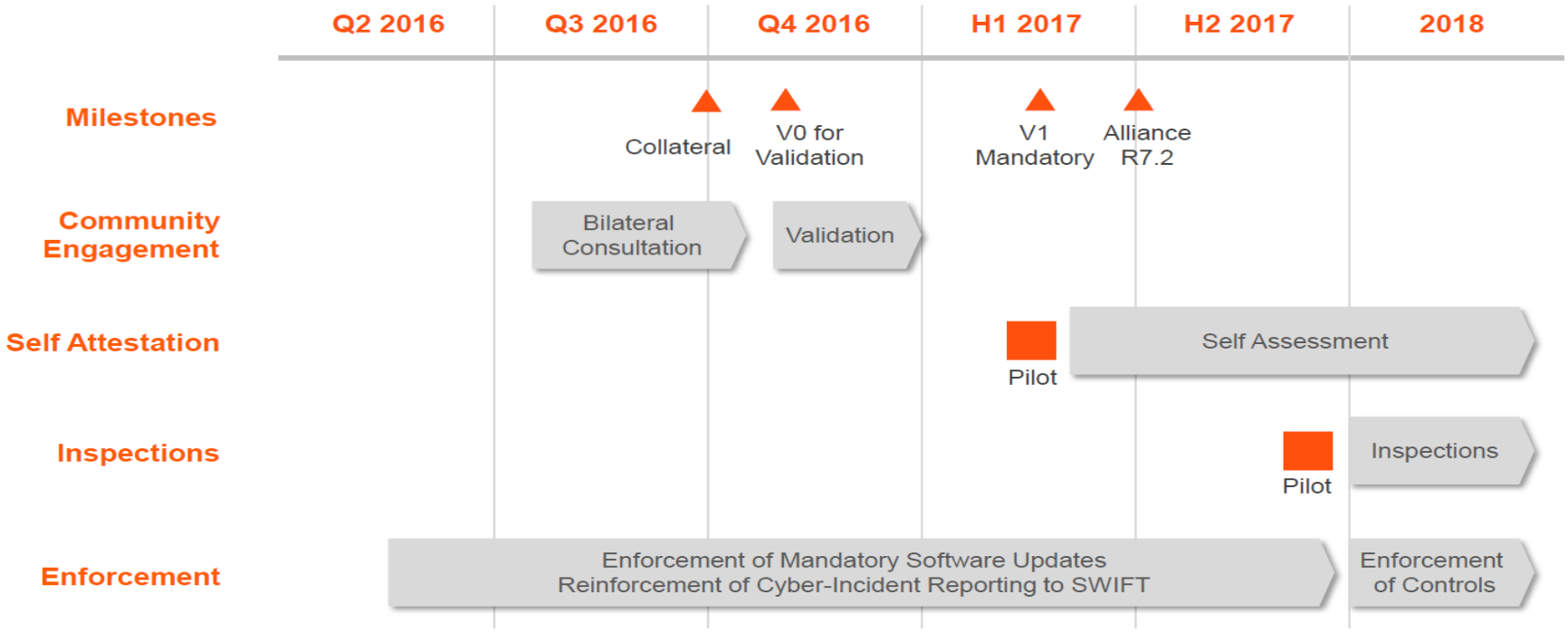
- December 2016 – Akbank **(Turkey)** - $4 million
- February 2016 - Bangladesh Central Bank **(Bangladesh)** - $81 million
- December 2015 – TP Bank (**Vietnam**) – Attempted $1.1 million
- January 2015 – Banco Del Austro / BDA (**Ecuador**) - $9 million

In addition, several successful hacks have not been announced due to risk of reputational loss.

In response to these SWIFT related attacks, SWIFT is introducing the Customer Security Program (CSP) which aims to improve information sharing throughout the community, enhance SWIFT-related tools for customers and provide audit frameworks.

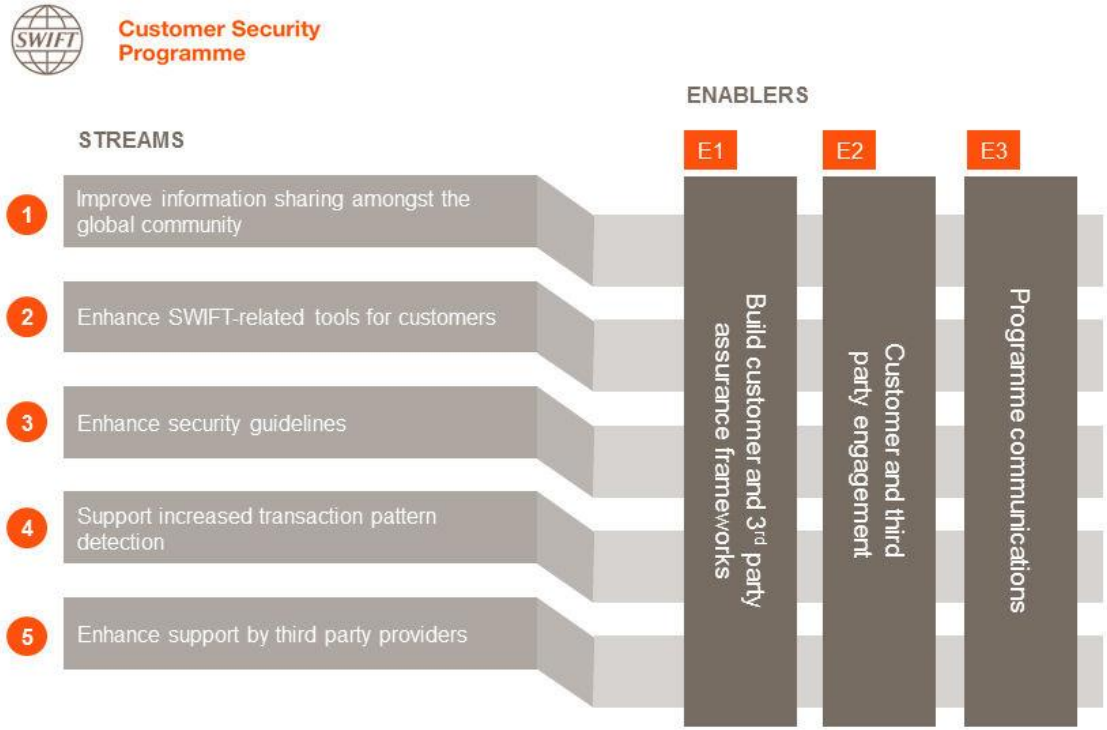
SWIFT CSP - Milestones

To ensure adoption, SWIFT will start requiring customers to provide detailed self-attestation against the mandatory controls from Q2 2017. Enforcement of mandatory requirements will start from January 2018, including inspections from internal and external auditors conducted with samples of customers to check quality.



SWIFT CSP - Overview

The Customer Security Program (CSP) incorporates five strategic initiatives, from facilitating better information sharing to creating new audit frameworks. These are intended to safeguard the security of the global banking system.



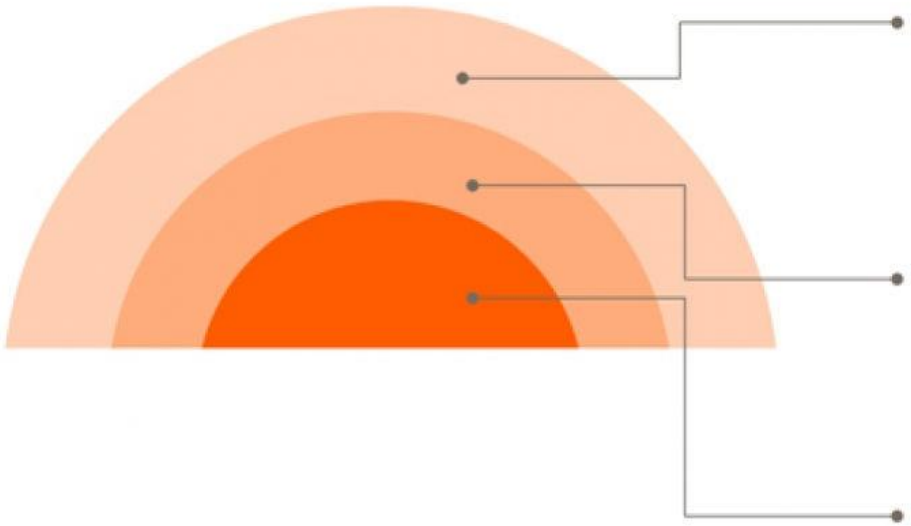
SWIFT Security Controls

This core set of requirements will apply to all SWIFT customers and are based around three objectives and eight principles described in the table below. 16 mandatory and 11 advisory controls will underpin the eight principles. The mandatory and advisory controls are described in the Appendix. A more detailed guideline that sets out how these controls are defined, should be applied, and will be measured via an assurance framework has also been published.

3 Objectives	8 Principles	27 Controls
Secure Your Environment	1. Restrict Internet access 2. Segregate critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment	• Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure • Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002 • Some controls are mandatory, some are advisory • Documentation and collateral will be available by end of October
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	

SWIFT Security Controls

Applying these standards will raise the security bar for customers on the SWIFT network and further support customers in their efforts to prevent and detect fraudulent use of their infrastructure. Implementation of these standards will also increase security awareness and education in the on-going fight against cyber-related wire fraud.



Self-Attestation

- Where customer positively asserts that it meets the security requirements
- First- and second-line of defence – provided by senior management

Self-Inspection

- Where customer's Internal Audit asserts that the customer meets the security requirements
- Third-line of defence - provided by IA function

Third-Party Inspection

- For an external party that provides independent validation that the customer meets the security requirements

How can KPMG Help

KPMG can assist its clients to comply with the SWIFT security requirements through providing them with a wide range of services.

Our services cover 1) review and report the clients' current controls in place for SWIFT security requirements, and 2) design and implement new frameworks and controls in order to assist clients in achieving the desired control state.

The SWIFT security assessment services offered by KPMG are:

- Attestation of the 16 mandatory and 11 optional SWIFT controls on behalf of clients
- Gap assessment of clients' current state and development of a target state roadmap
- Review clients' Cyber Security framework and propose additional improvements
- Assess the current IT controls in place in accordance with SWIFT security requirements
- Develop and implement an Information Sharing Framework
- Establish Enhanced Transaction Pattern detection & Data Analytics
- Selection and implementation of SWIFT and third party security tools
- Penetration testing of all related SWIFT applications and interfaces (grey-box)

KPMG has been involved in many client engagements within the financial industry and corporates. We performed many security reviews, security assessments, IT audits, penetration tests and ethical hacking engagements (red-teaming) on Swift implementations and related back-office systems. Credentials are available at request.

KPMG would welcome the opportunity to further explain its services suite.

KPMG

Appendix

SWIFT Customer Security Program Controls

SWIFT Security Controls

Mandatory Controls (16)

1. Restrict Internet Access and Segregate Critical Systems from General IT Environment	
1.1 SWIFT Environment Segregation	A segregated secure zone safeguards the local SWIFT infrastructure from compromises and attacks from the broader enterprise and external environment.
1.2 Operating System Privileged Account Control	Access to local operating system accounts with system-level administrative rights 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, the accounts are restricted from being accessed.

2. Reduce Attack Surface and Vulnerabilities	
2.1 Internal Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT data flows within the secure zone, and its link to the user PCs.
2.2 Security Updates	All hardware and software inside the secure zone and on user PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.
2.3 System Hardening	Security hardening is conducted on all systems and infrastructure within the secure zone and on user PCs.

3. Physically Secure the Environment	
3.1 Physical Security	Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

SWIFT Security Controls

Mandatory Controls (16)

4. Prevent Compromise of Credentials	
4.1 Password Policy	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts.
4.2 Multi-factor Authentication	Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.

5. Manage Identities and Segregate Privileges	
5.1 User Account Management	Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties.
5.2 Token Management	Authentication tokens are managed appropriately during issuance, revocation, use, and storage.

6. Detect Anomalous Activity to Systems or Transaction Records	
6.1 Malware Protection	Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.
6.2 Software Integrity	A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications.
6.3 Database Integrity	A database integrity check is performed at regular intervals on databases that record SWIFT transactions.
6.4 Logging and Monitoring	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs.

SWIFT Security Controls

Mandatory Controls (16)

7. Plan for Incident Response and Information Sharing	
7.1 Cyber Incident Response Planning	The organisation has a defined cyber incident response plan.
7.2 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 Controls (11)

2. Reduce Attack Surface and Vulnerabilities	
2.4A Back Office Data Flow Security	Confidentiality, integrity, and authentication mechanisms are implemented to protect data flows between back office systems or middleware and the secure zone.
2.5A External Transmission Data Protection	Sensitive data leaving the secure zone is encrypted.
2.6A User Session Integrity	The integrity and confidentiality of interactive user sessions connecting to the secure zone are safeguarded.
2.7A Vulnerability Scanning	Vulnerability scanning is conducted within the secure zone and on user PCs using an up-to-date industry-standard scanning tool.
2.8A Critical Activity Outsourcing	Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.
2.9A Transaction Business Controls	Restrict transaction submission and receipt to the expected bounds of normal business.

SWIFT Security Controls

Advisory Controls (11)

5. Manage Identities and Segregate Privileges	
5.3A Personnel Vetting Process	Staff operating the locally hosted SWIFT infrastructure are vetted prior to initial employment in that role and periodically thereafter.
5.4A 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.
6. Detect Anomalous Activity to Systems or Transaction Records	
6.5A Intrusion Detection	Intrusion detection is implemented to detect unauthorised network access.
7. Plan for Incident Response and Information Sharing	
7.3A Penetration Testing	Application, host, and network penetration testing is conducted at least annually within the secure zone and on user PCs.
7.4A 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.

kpmg.bm