www.pwc.ch/cybersecurity

SWIFT
Customer Security Programme

Mandatory controls: what you have to do to protect your local SWIFT infrastructures

pwc

SWIFT Customer Security Programme (CSP)

The growing number of cyber-attacks, including those on local SWIFT infrastructures, has prompted SWIFT to define mandatory controls for SWIFT participants to fight cyber threats.

In May 2017 the Society for Worldwide Interbank Financial Telecommunication (SWIFT) augmented its Customer Security Programme (CSP) with the publication of a set of Customer Security Controls defining specific requirements to be met by all SWIFT participants.

The programme aims to improve the exchange of information within the SWIFT community, ensure a high level of security at local SWIFT infrastructures run by participants, put in place an assurance framework to counter the ever-increasing number of cyber-threats, and strengthen the ability of SWIFT participants to combat cyber-attacks.

Recent attacks on the SWIFT network

On 4 and 5 February 2016, attackers who had compromised systems at the Bangladesh Central Bank sent a number of payment instructions over its interface with the SWIFT network. These payment instructions totalled USD 951 million, of which USD 101 million was processed by the Federal Reserve Bank of New York. The fraudsters were able to launder USD 81 million of the money (largely through casinos in the Philippines). USD 20 million was recovered after it was diverted to Sri Lanka.

This and other recent cyber-attacks show that attackers are not targeting the SWIFT network itself, but exploiting the security weaknesses of an institution's local infrastructure. While customers are responsible for protecting their own IT environments and access to SWIFT, the introduction of the SWIFT CSP is designed to help customers in the fight against cyber fraud.

Step 0
Cyber attack on a bank's IT environment

Step 1
How does it work?
Attackers analyse payment systems and processes

Step 2
Who does what?
Attackers analyse the different actors in the payment processes

Step 3
How do I act like them?
Attackers obtain valid operator credentials

Step 4
Fraud
Attackers submit fraudulent messages

Objectives, principles and controls

The CSP calls upon all SWIFT participants to implement a control and assurance framework consisting of 16 mandatory and 11 advisory security controls. The controls are based on existing SWIFT security guidelines and are in line with good practice standards such as NIST, ISO/IEC 27002 and PCI-DSS. The mandatory controls establish a security baseline for the entire SWIFT community. SWIFT also recommends implementing the advisory controls to optimally protect local SWIFT infrastructures.

Objectives	Principles	Controls
Secure your environment	Restrict internet access and protect critical systems from general IT environment	27 controls: • 16 mandatory • 11 advisory The applicability to the local SWIFT infrastructure depends on the architecture. Not all controls are applicable to architectures without local, SWIFT-specific components.
	Reduce attack surface and vulnerabilities	
	Physically secure the environment	
Know and limit access	Prevent compromise of credentials	
	Manage identities and segregate privileges	
Detect and respond	Detect anomalous activity in systems or transaction records	
	Plan for incident response and information sharing	

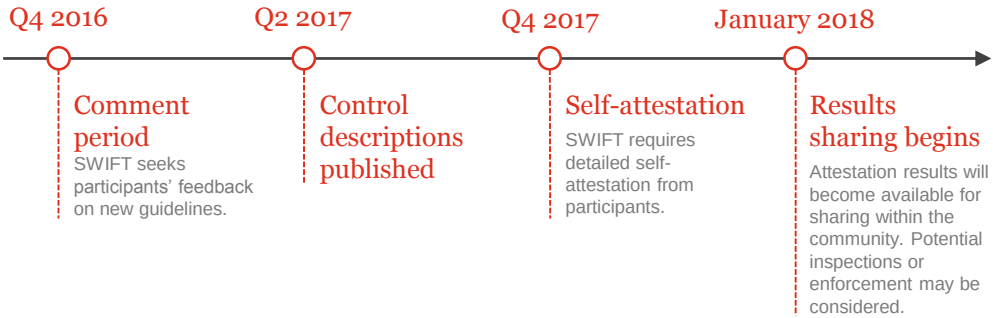
What action do I need to take?

The SWIFT CSP will come into force on 1 January 2018. Before the introduction of the programme, each SWIFT participant must conduct a self-assessment and notify SWIFT of its compliance status in terms of the controls by the end of 2017. From 2018, all participants must confirm their compliance with the controls annually. This confirmation can be provided via a self-assessment (self-attestation), internal audit (self-inspection) or an external audit (third-party inspection). SWIFT will also carry out regular spot-checks of confirmations, by means of internal or external audits, for quality assurance purposes.

What happens if I don't comply?

If your organisation fails to comply with these new requirements, SWIFT can report this to your local supervisory authority. Failures to submit a self-attestation, or late submission, will be reported starting 2018, and non-compliance with the mandatory controls will be reported from 2019. SWIFT will also report non-compliance to other counterparties if there is no direct local supervisory authority for your organisation.

It is therefore crucial to perform the self-assessment as quickly as possible, and to send your self-attestation or confirmation of inspection of compliance every year.



Looking beyond the mandatory controls

SWIFT participants should begin now to anticipate the threat class behind the Bangladesh Central Bank cyber-attack, and not wait until they are attacked. Organisations should examine and investigate their current environment – beyond the traditional security-log analysis – to determine whether they have already been attacked, or at least targeted, by this threat actor.

Institutions should also prepare for oncoming attacks as this threat scheme adapts and additional threat actors attempt to replicate its original success.

PwC's threat intelligence service offering helps you maintain an up-to-date view of the threats relevant to your organisation and detect persistent and ongoing intrusions.

How PwC can help

SWIFT Readiness Assessment

We can help make sure you comply with the SWIFT CSP requirements by 1 January 2018 by assessing your current status and highlighting any gaps.

Outcome: A complete overview of your implemented controls and the gaps you need to close to become compliant.

SWIFT controls implementation and support

We can help you implement controls or perform a post-implementation review to enable your organisation to comply with the SWIFT CSP requirements.

Outcome: A tailored roadmap to achieving compliance, personalised assistance in the implementation of strategies, processes and technologies, and a security review of your implemented controls.

SWIFT compliance confirmation

We can assist you with your annual confirmation of compliance with the SWIFT CSP requirements.

Outcome: An assessment confirming your compliance with the SWIFT CSP, recognised by SWIFT as a third-party inspection.

Threat intelligence and detection

We can help you keep an up-to-date view of threats to your organisation and detect persistent and ongoing intrusions.

Outcome: Quarterly reports on the cyber-threat landscape specific to your sector, in-person briefings, monitoring and alerts of specific threats, and an incident response retainer.

We can also help your organisation with the following services:

- Data classification, governance, compliance and protection
- Identity and access management strategy and implementation
- Incident response and forensics
- IT security architecture
- Penetration tests
- Regulatory compliance
- Threat and vulnerability management

... are you ready?

For more information, please visit us at www.pwc.ch/cybersecurity

or contact us directly:

Reto Häni
Cyber Security Partner and Leader

PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Yan Borboën
Cyber Security Partner

PwC Assurance
+41 79 580 73 53
yan.borboen@ch.pwc.com

Jens Probst
Systems & Process Leader

PwC Assurance
+41 58 792 29 59
jens.probst@ch.pwc.com

Nicolas Vernaz
Data Protection and Regulatory Compliance Leader

PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com

We've done this before

PwC offers a truly global cybersecurity service, with over 3,200 professionals worldwide, enabling us to tap into a global network and deliver value locally – wherever you are operating.

Our full range of services includes technical, business and legal expertise to help you navigate the challenges and threats faced by business today – at the technical level as well as at board level.

pwc