RO SWIFT Business Forum 2017

Customer Security Programme (CSP)

Michael Formann, Head of SWIFT Germany and Austria

Bucharest, 8.11.2017

CSP update

(Customer Security Programme)

IR 764
March 2017

Modus Operandi

Step 1

Attackers compromise customer's environment

Step 2

Attackers obtain valid operator credentials

Step 3

Attackers submit fraudulent messages

Step 4

Attackers hide the evidence

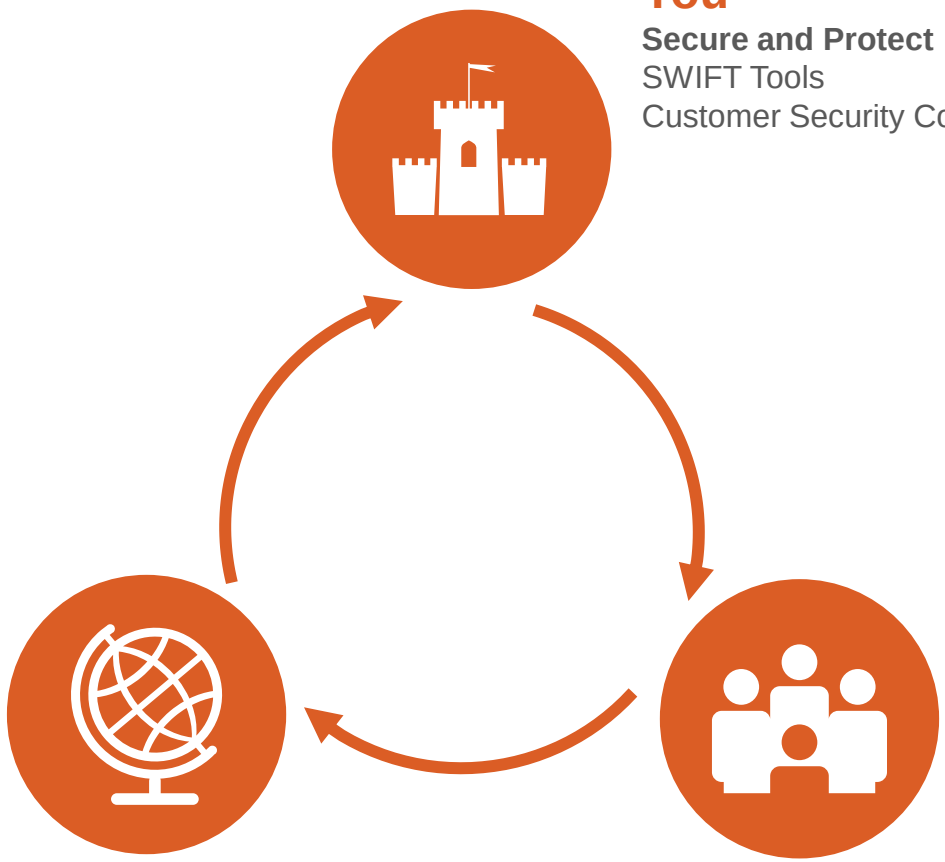
- Attackers are well-organised and sophisticated
- Common starting point has been a security breach in a customer’s local environment
- There is no evidence that SWIFT’s network and core messaging services have been compromised

Customer Security Programme (CSP)

SWIFT launched the Customer Security Programme to help customers **reinforce the security of the global banking system.**

You

Secure and Protect
SWIFT Tools
Customer Security Controls Framework



Your Counterparts

Prevent and Detect
Transaction Pattern Detection – RMA, DVR and Payment Controls

Your Community

Share and Prepare
Intelligence Sharing
SWIFT ISAC Portal

CSP | Your Counterparts > RMA & RMA Plus

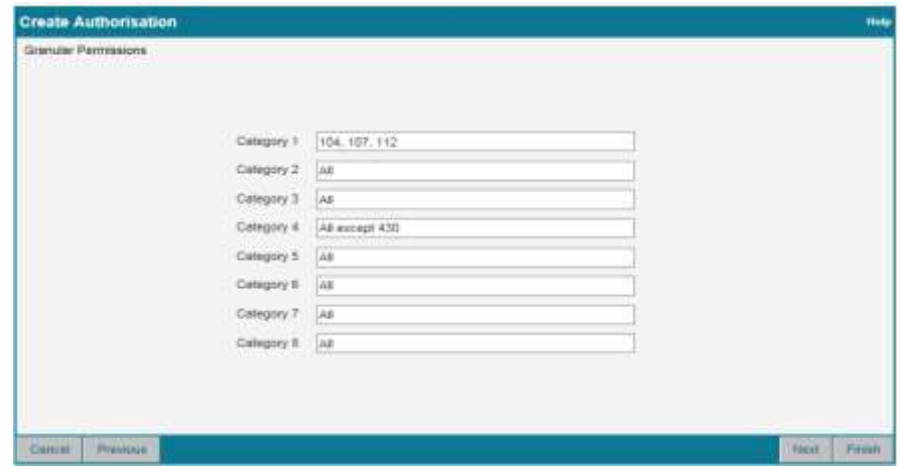
RMA

You control who can send you authenticated SWIFTNet FIN traffic at BIC8 level

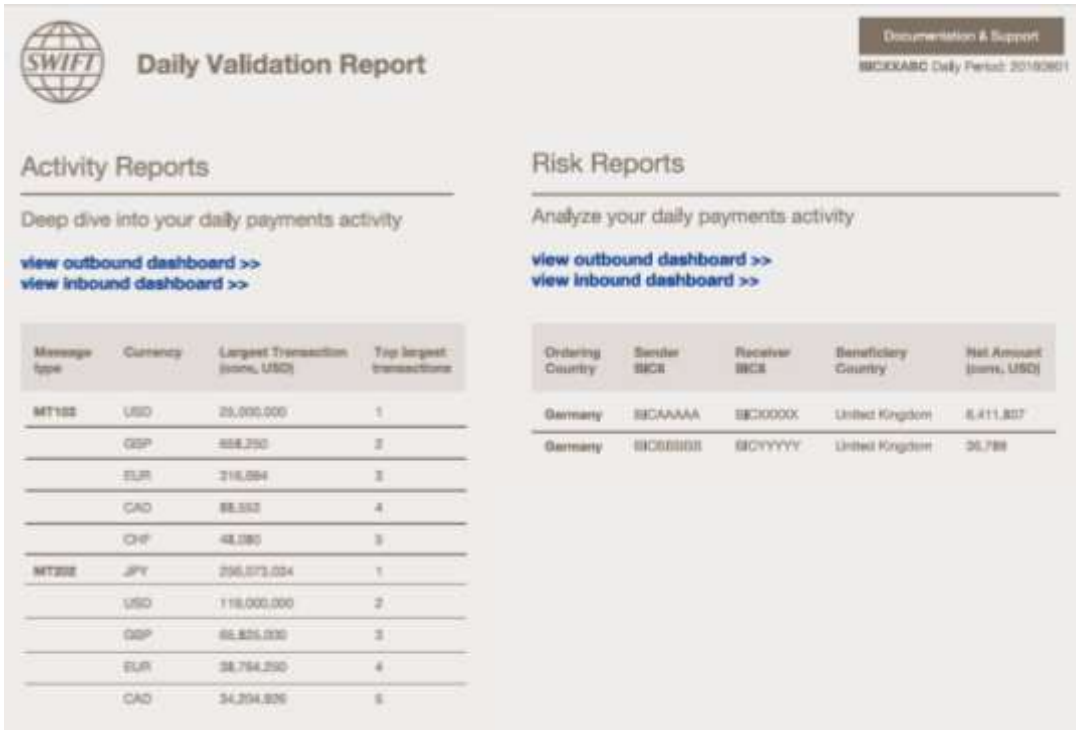
RMA Plus (optional)

You control what a correspondent can send you

- Category of business your correspondents are allowed to send you
- Unwanted messages blocked at the sender level
- One-way relationship management
  - **Even** if your correspondent does not have the RMA Plus option



CSP | Your Counterparts > Daily Validation Report



Daily Validation Report

Documentation & Support

Activity Reports

Deep dive into your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Message type	Currency	Largest Transaction (conv. USD)	Top largest transactions
MT103	USD	20,000,000	1
	GBP	658,250	2
	EUR	216,084	3
	CAD	88,552	4
	CHF	48,080	5
MT202	JPY	296,073,024	1
	USD	119,000,000	2
	GBP	66,825,030	3
	EUR	38,764,250	4
	CAD	34,204,826	5

Risk Reports

Analyze your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Ordering Country	Sender BIC8	Receiver BIC8	Beneficiary Country	Net Amount (conv. USD)
Germany	BICAAAAA	BICXXXXX	United Kingdom	8,411,807
Germany	BICBBBBB	BICYYYYY	United Kingdom	36,788

Activity Reports | Aggregate Daily Activity

- Message type
- Currency
- Country
- Counterparties

- Daily volume total
- Daily value total
- Maximum value of single transactions
- Comparisons to daily volume and value averages

Risk Reports | Large or Unusual Message Flows Based on Ordered Lists

- Largest single transactions
- Largest aggregate transactions for counterparties
- New counterparty relationships

You | Helping customers to secure and protect their local environments

1. SWIFT Customer Security Controls Framework

2. Customer Security Attestation Process

3. Specific interface and third party security guidance documents

4. Reinforcement of SWIFT tools

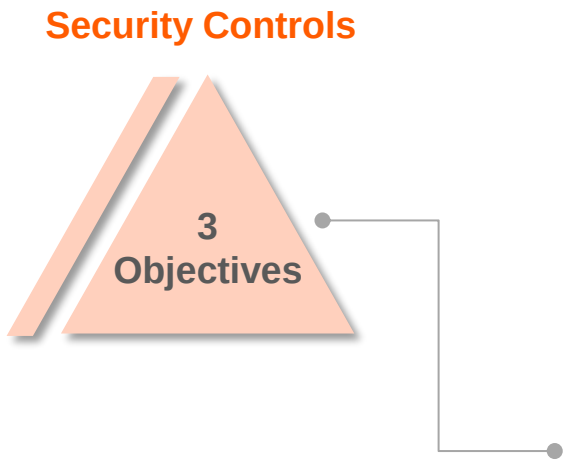
Customer Security Controls Framework
SWIFT is creating a security baseline

SWIFT has introduced a core set of security controls that every SWIFT customer must implement.

We are making these security controls **mandatory** for all customers to set a **security baseline** for the whole industry.

You will need to **implement the controls that are relevant to your organisation**, and attest your level of compliance **before the end of 2017**.

SWIFT Customer Security Controls Framework
3 Objectives



1. Secure Your Environment

Secure your environment from cyber attacks

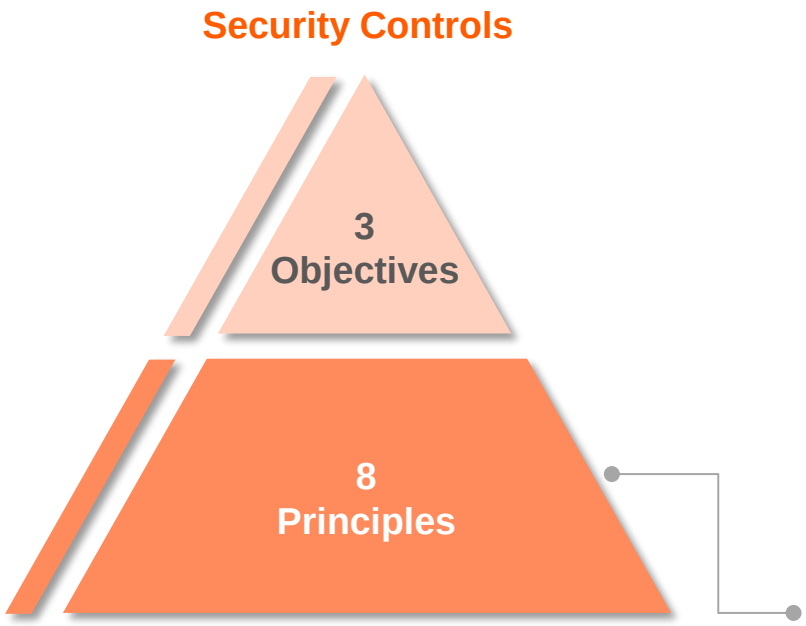
2. Know and limit access

Know and **limit access of people** to the local SWIFT environment

3. Detect and respond

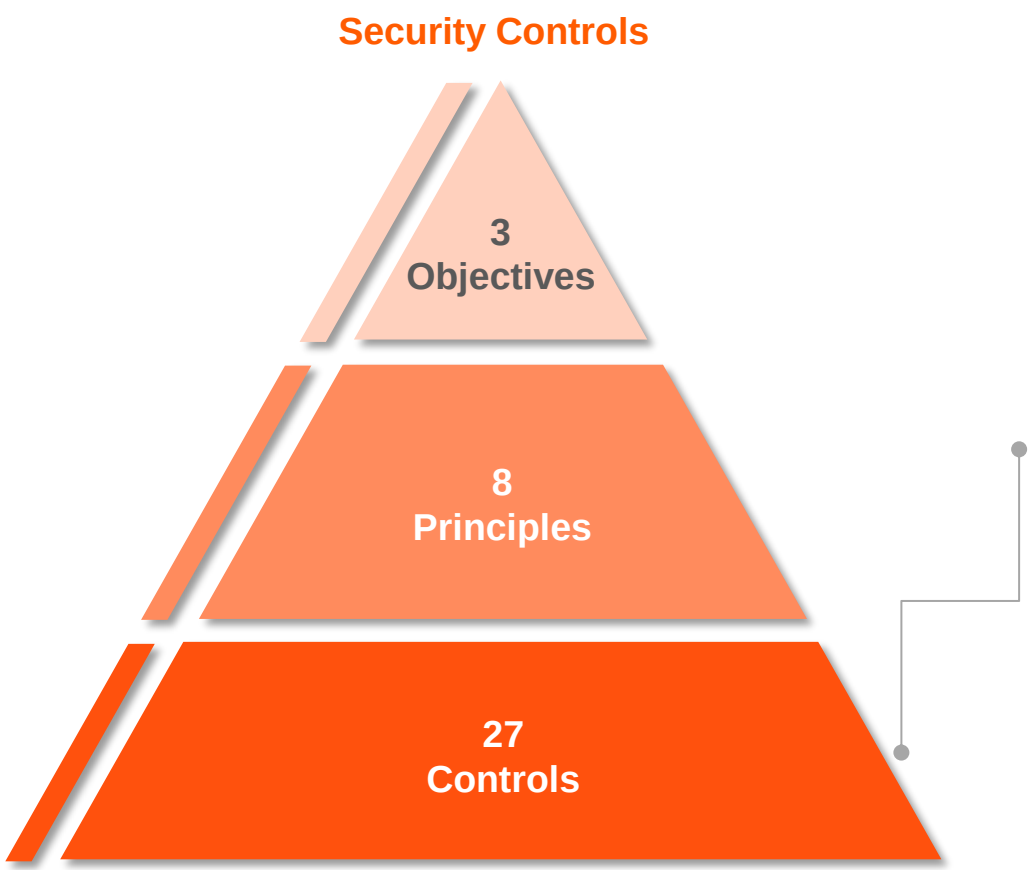
Promptly **detect and respond** in case of a cyber attack

SWIFT Customer Security Controls Framework
8 Principles



SWIFT Customer Security Controls Framework		
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
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 Customer Security Controls Framework
27 Controls



The 8 security principles are put into practice with 27 controls. **16 mandatory, 11 advisory.**

- in line with existing information security industry standards, and product-agnostic.
- expected to evolve over time in light of the changing cyber-threat landscape

Mandatory security controls

- establish a security baseline for the entire community
- all users must self-attest against their implementation on their local SWIFT-related infrastructure.
- set a realistic goal for near-term, tangible security gain and risk reduction.

Advisory controls

- based on good practice that SWIFT recommends customers implement on their local SWIFT-related infrastructure.

Customer Security Attestation Process (CSAP): Four Main Steps

1. Submission of self-attestation

2. Grant access to counterparties

3. Follow-up activities to drive compliance and improve security

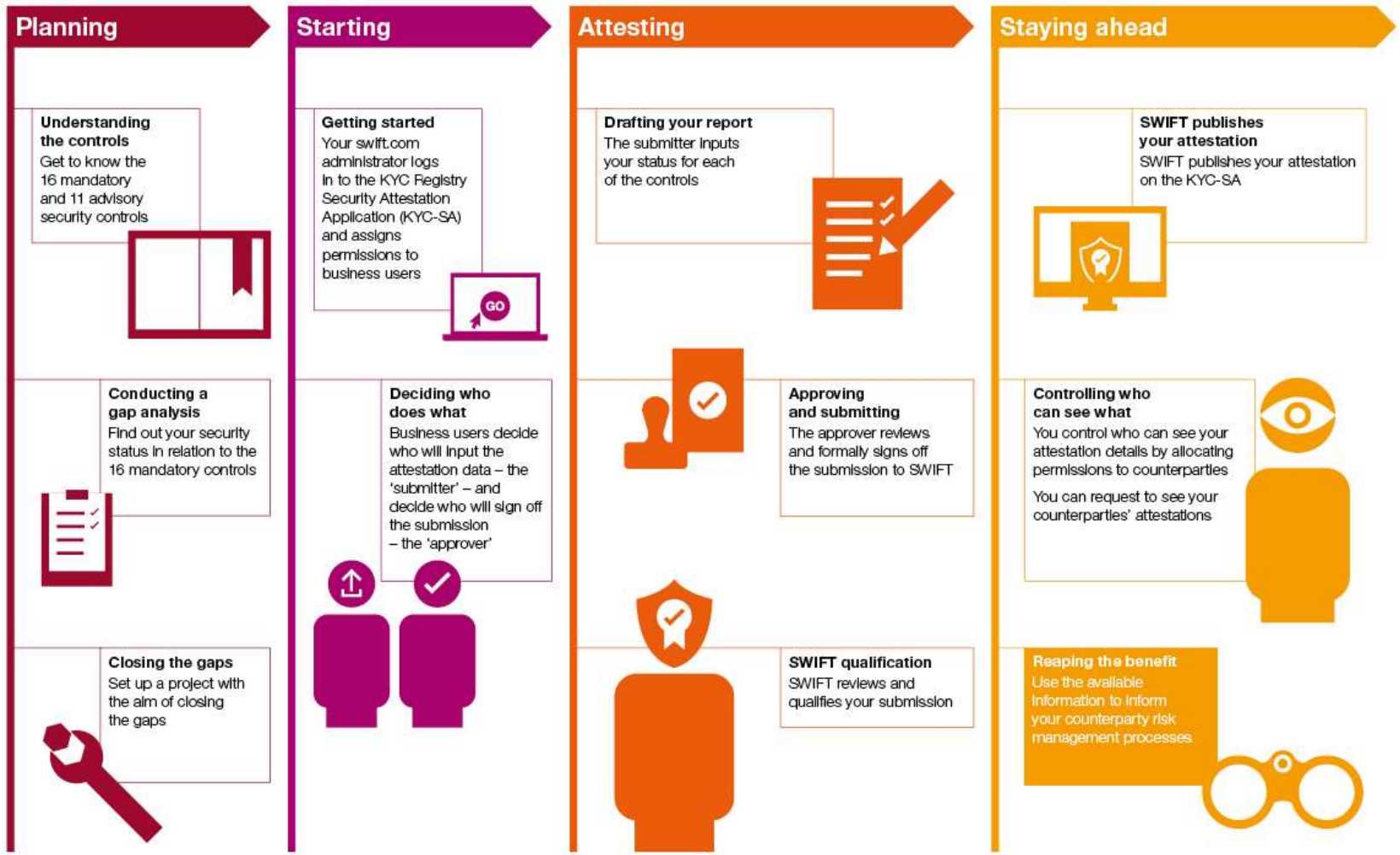
4. Quality checks through sample requests for internal or external audit reports

Customer Security Programme
Attestation Process

SWIFT's Customer Security Programme sets the baseline that reinforces the security of the global financial community.

Self-attest against the security controls by 31 December 2017.

For additional information go to swift.com/csp



Additional Community Support > via SWIFT and Third Party providers

Third party providers

3rd Party Security Consultants – an ecosystem of vendors

Via SWIFT

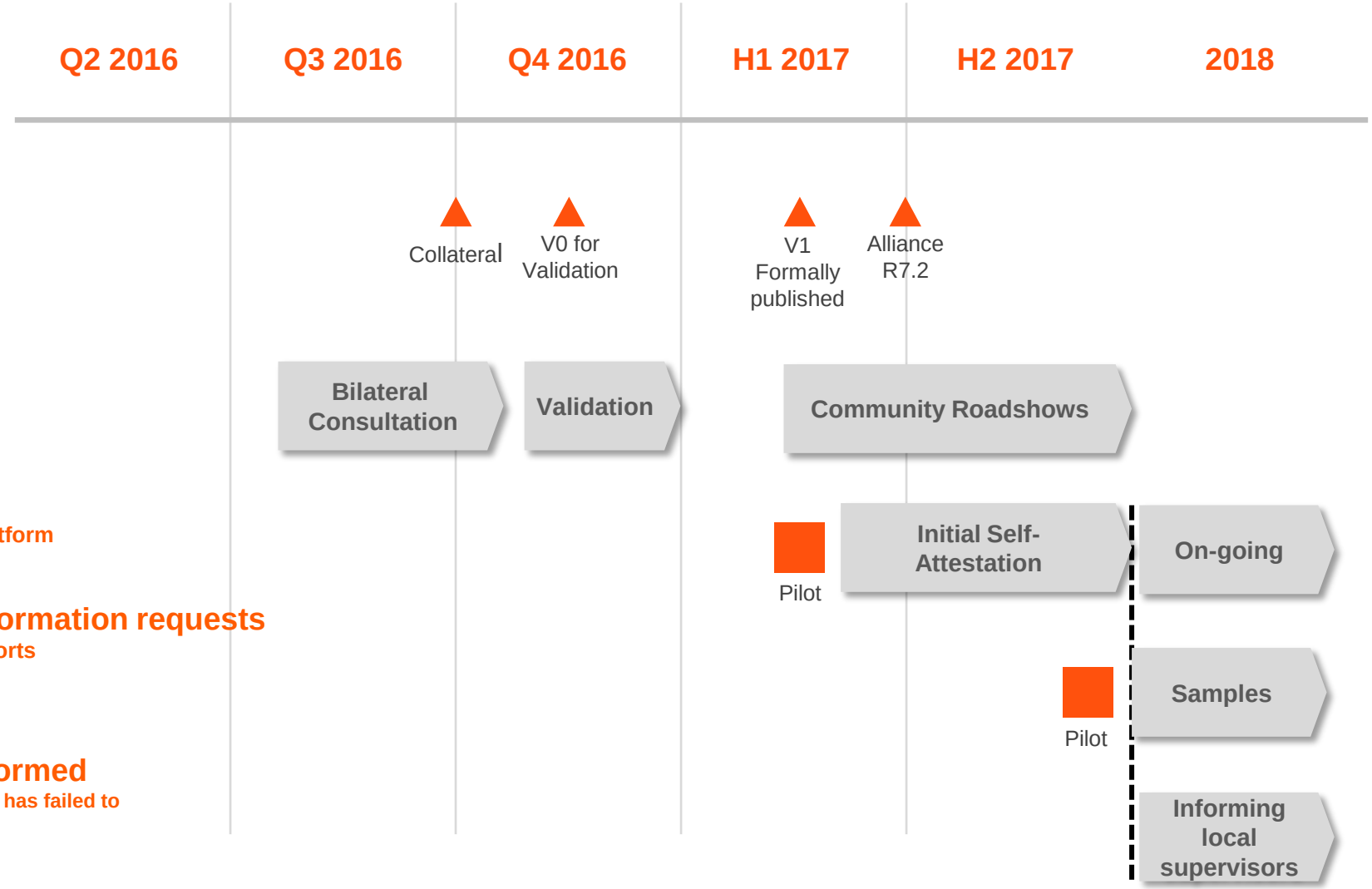
mySWIFT – Evolution of self-service on-demand support

24/7 Customer Support – CSP specialists & local experts

SWIFTSmart Interactive training

Documentation – Security Controls Framework, Attestation Policy, FAQs

Timeline


Q2 2016
Q3 2016
Q4 2016
H1 2017
H2 2017
2018
Security Controls Framework
Collateral
V0 for Validation
V1 Formally published
Alliance R7.2
Community Engagement
Bilateral Consultation
Validation
Community Roadshows
Self-Attestation
Via security folder on KYC platform
Pilot
Initial Self-Attestation
On-going
Additional sample information requests
Eg -internal/external audit reports
Samples
Pilot
Local supervisors informed
Of any supervised institution that has failed to submit an attestation
Informing local supervisors

To get the message clear:

Deadline 1: now – get started setting up the self-attestation tool

Deadline 2: 31.12.2017 – self attestation to be submitted – irrespective of status

Deadline 3: 31.12.2018 – self attestation of full compliance


The global provider
of secure financial messaging services
Security notice
日本語 | Languages | 中文
Ordering & Support
About Us
Your Needs
Our Solutions
Standards
News & Events
Join SWIFT
Contact Us
mySWIFT
Home › mySWIFT › Customer Security Programme (CSP)
Customer Security Programme (CSP)
Reinforcing the security of the global banking system
Programme description ›
Contact us ›
Subscribe to security notifications
Overview
Programme description
Security announcements
Security controls
Training
Document centre
Contact us
Safeguarding security across the banking community
The growing threat of cyberattacks has never been more pressing. Recent instances

Questions and
open discussion