Customer Security Program - supporting the community in strengthening security

September 12, 2017

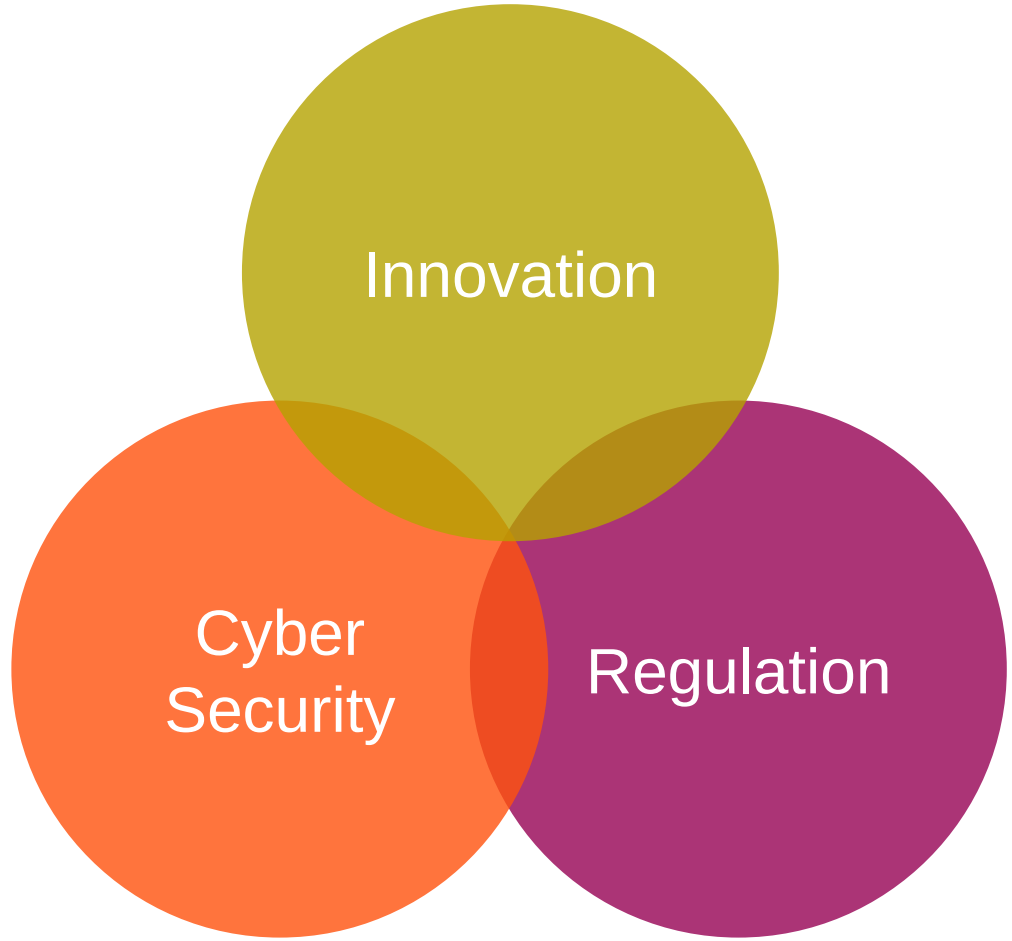
Juan Martinez, Head of Latin America and Caribbean region - SWIFT

The global provider of secure financial messaging services

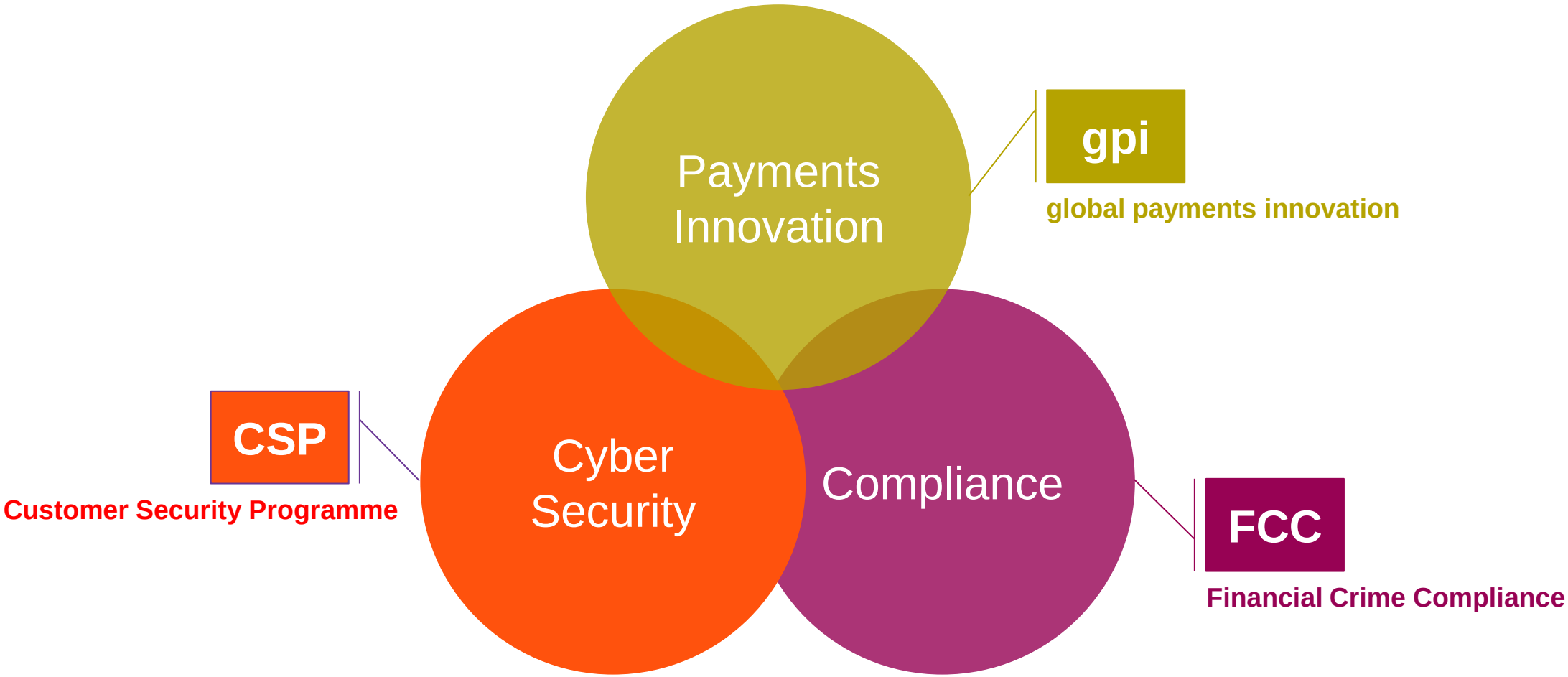
SWIFT in figures

Industry Change & Challenges

The traditional model is undergoing rapid change, driven by innovation, cyber security and regulation



SWIFT is leading 3 initiatives, that combined take correspondent banking to the next level



Customer Security Programme (CSP)

CSP | 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 (still) no evidence that SWIFT’s network and core messaging services have been compromised

CSP | Programme Overview

You

Secure and Protect

SWIFT Tools
Security Guidelines and Assurance

Your Community

Share and Prepare

Intelligence Sharing

Your Counterparts

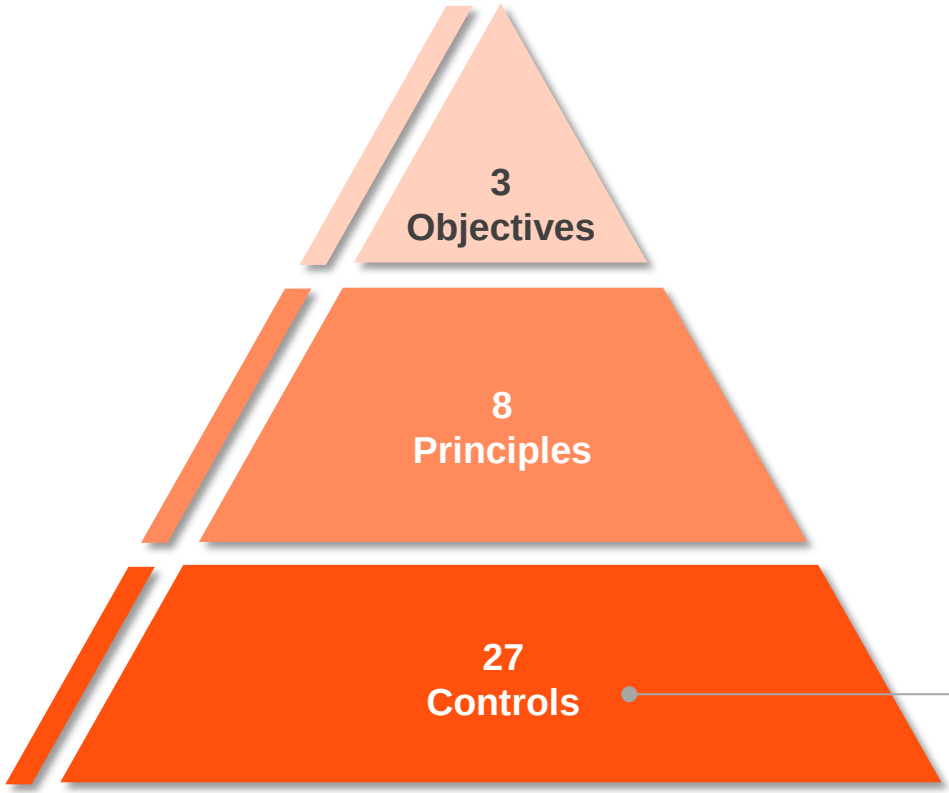
Prevent and Detect

Transaction Pattern Detection – RMA, DVR and Payment Controls

Launched on May 27th 2016, CSP supports all customer segments, whether directly or indirectly connected, in reinforcing the security of their SWIFT-related infrastructure

CSP | You > Security Guidelines and Assurance

Security Controls

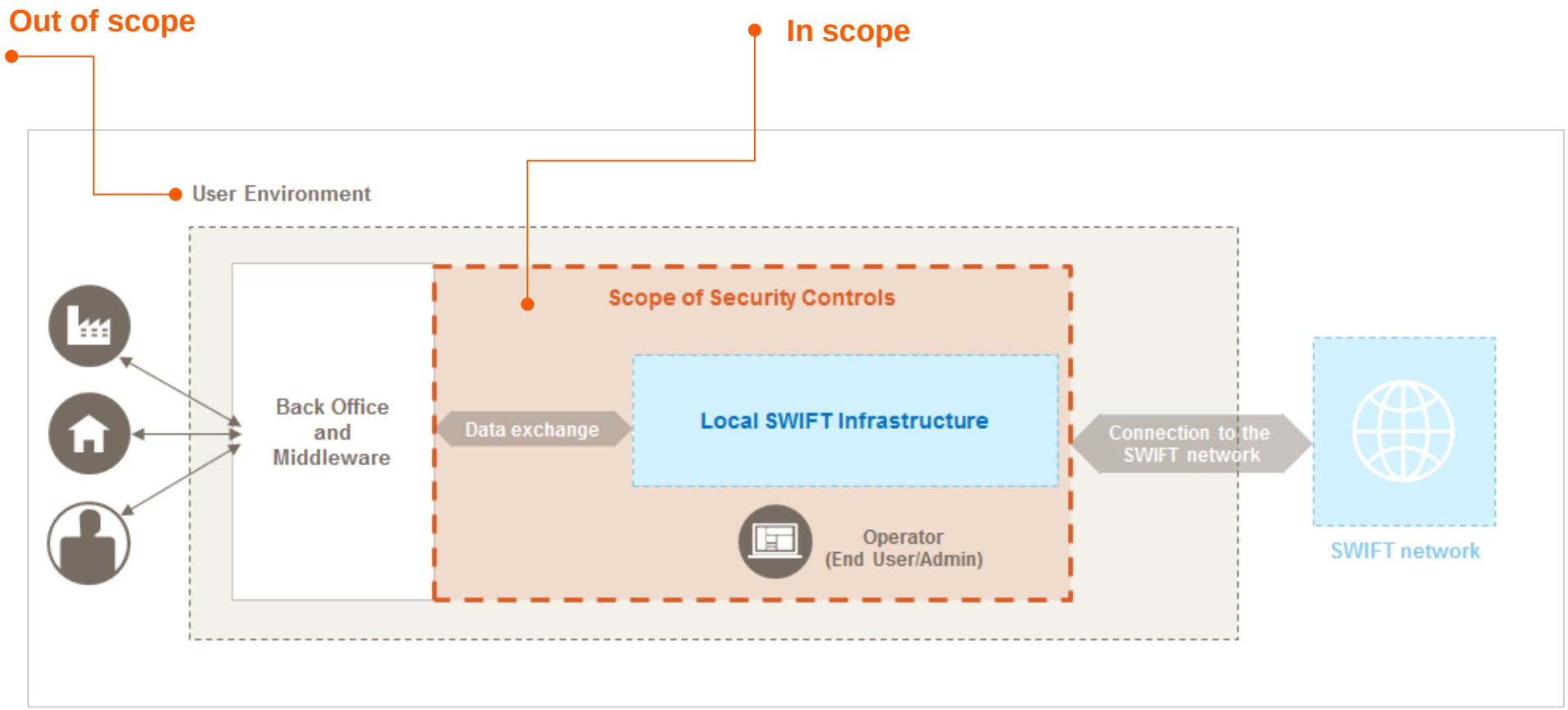


CSP Security Controls Framework

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

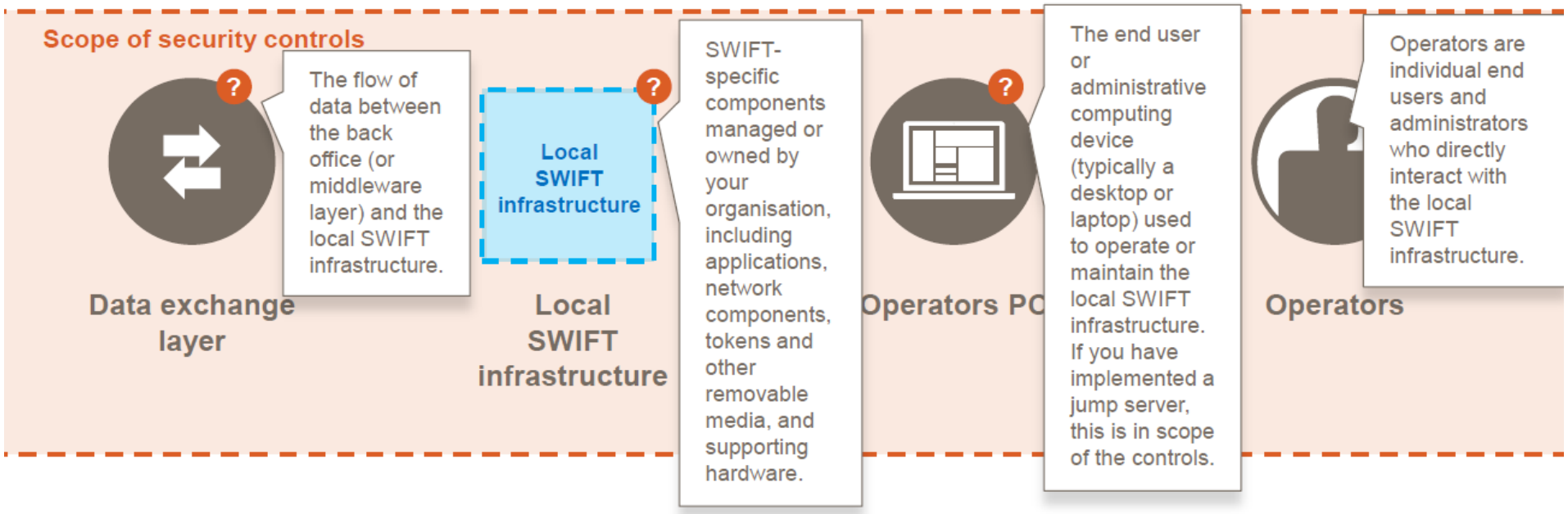
- *Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure*
- *Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002*
- *16 controls are mandatory, 11 are advisory*
- *Final version published March 31, 2017*

CSP | You > Security Guidelines and Assurance
Scope of the Controls



CSP | You > Security Guidelines and Assurance

Scope of the Controls



CSP | You > Security Guidelines and Assurance
Controls Framework

The SWIFT Customer Security Controls Framework document

To comply with a relevant control you need to:

- **meet the control objective**
- **address the defined risk drivers**
- **cover the specified scope**

Type A
Control Number and Title 1.2 Operating System Privileged Account Control
Control Type Mandatory
Control Objective Restrict and control the allocation and usage of administrator-level operating system accounts.
In Scope Components – Messaging interface – Communication interface – …
Risk Drivers – Unauthorised administrative access – Password compromise – Deletion of activity evidence (e.g., logs)
Implementation Guidance <Guidance details>

CSP | You > Security Guidelines and Assurance
Controls Framework

The SWIFT Customer Security Controls Framework document

Check here if the control applies to your organisation's architecture type.

Type A

In this example, "1." stands for principle number one: *Restrict Internet access and protect critical systems from general IT environment*. "2" stands for the control number two of this principle. If the control is not mandatory it will add the letter "A" (Advisory). For example 6.5A (principle 6, control 5, advisory).

Control Number and Title
1.2 Operating System Privileged Account Control

This section says if the control is mandatory or advisory.

Control Type
Mandatory

Control Objective
Restrict and control the allocation and usage of administ accounts.

This is the security goal to be achieved irrespective of the implementation method. You can implement the solution that best fits your environment, as long as it complies with the defined control objective.

The components in scope for this particular control (for example: Messaging interface, Communication interface, data exchange layer).

In Scope Components
- Messaging interface
- Communication interface
- …

Risk Drivers
- Unauthorised administrative access
- Password compromise
- Deletion of activity evidence (e.g., logs)

The risks this control aims to mitigate. This helps you to evaluate the solutions you will apply. Some risk drivers are the same for multiple controls.

You must implement a solution that meets the control objective. This is the SWIFT-formulated method for control implementation.

Implementation Guidance
<Guidance details>

CSP | You > Security Guidelines and Assurance
Controls

Mandatory and Advisory Security Controls	A	B
1 Restrict Internet Access and Protect Critical Systems from General IT Environment		
1.1 SWIFT Environment Protection	•	
1.2 Operating System Privileged Account Control	•	
2 Reduce Attack Surface and Vulnerabilities		
2.1 Internal Data Flow Security	•	
2.2 Security Updates	•	•
2.3 System Hardening	•	•
2.4A Back-office Data Flow Security	•	•
2.5A External Transmission Data Protection	•	
2.6A Operator Session Confidentiality and Integrity	•	•
2.7A Vulnerability Scanning	•	•
2.8A Critical Activity Outsourcing	•	•
2.9A Transaction Business Controls	•	•
3 Physically Secure the Environment		
3.1 Physical Security	•	•
4 Prevent Compromise of Credentials		
4.1 Password Policy	•	•
4.2 Multi-factor Authentication	•	•

Mandatory and Advisory Security Controls	A	B
5 Manage Identities and Segregate Privileges		
5.1 Logical Access Control	•	•
5.2 Token Management	•	•
5.3A Personnel Vetting Process	•	•
5.4A Physical and Logical Password Storage	•	•
6 Detect Anomalous Activity to Systems or Transaction Records		
6.1 Malware Protection	•	•
6.2 Software Integrity	•	
6.3 Database Integrity	•	
6.4 Logging and Monitoring	•	•
6.5A Intrusion Detection	•	
7 Plan for Incident Response and Information Sharing		
7.1 Cyber Incident Response Planning	•	•
7.2 Security Training and Awareness	•	•
7.3A Penetration Testing	•	•
7.4A Scenario Risk Assessment	•	•

CSP | You > Security Guidelines and Assurance

Supporting the Community

Guidance on the Customer Security Controls Framework

SWIFT Support

SWIFT guidance on the customer security controls framework

Customer security work session

Hundreds of work sessions held in local communities and via Webinars to share CSP milestones and deliverables

CSP pages

Visit the CSP pages for programme news and updates

The SWIFT Customer Security Controls Framework and Security Controls Policy Document

Review the SWIFT Customer Security Controls Framework and the Security Controls Policy Document.

Customers must log in to mySWIFT with their swift.com credentials to access the documents.

SWIFTSmart

The SWIFTSmart e-learning training platform includes a portfolio of modules, including in-depth modules on each of the mandatory security controls

MySWIFT

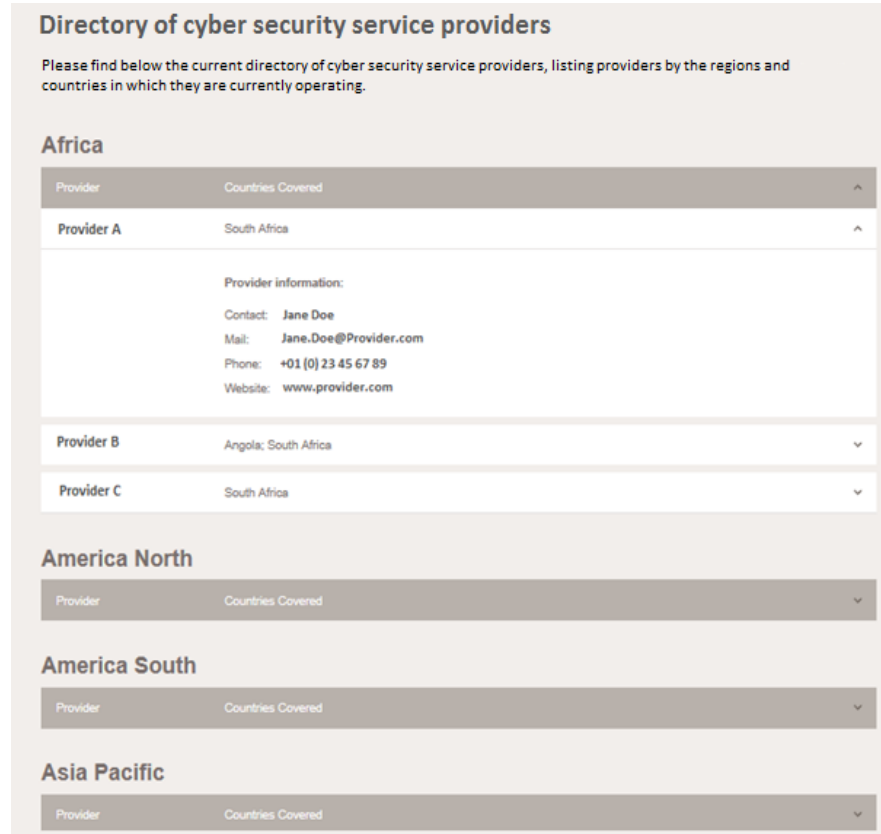
MySWIFT A self-service portal containing “how-to’ videos, guidance on frequently asked questions and Knowledge Base tips.

CSP | You > Security Guidelines and Assurance
Directory of Cyber Security Service Providers

If customers need assessment or implementation support, they can consult the directory of cyber-security service providers on SWIFT.com to help find a suitable third-party project partner

- The Directory of Cyber Security Providers is for SWIFT customers' reference only
- SWIFT does not endorse or warrant the providers (or their services) listed in the Directory
- SWIFT users can opt to contract with other providers that are not featured in the Directory
- **SWIFT users must always conduct their own analysis of the suitability of a Cyber Security Service Provider for their purposes**

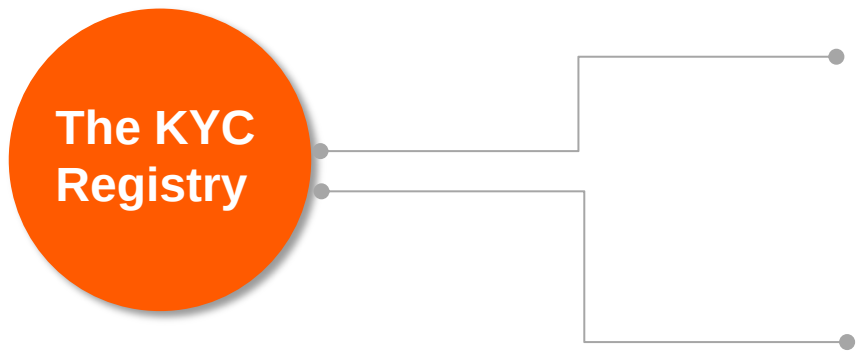
Available on SWIFT.com/CSP



CSP | You > Security Guidelines and Assurance
Attestation

Builds on the principles of fostering transparency between users and ensuring customers remain in control.

- Central tool to submit self-attestation status information
- Attesting user remains in control of publication of its data to counterparties
- Any other user must request access to the attesting user to view its data



A central tool

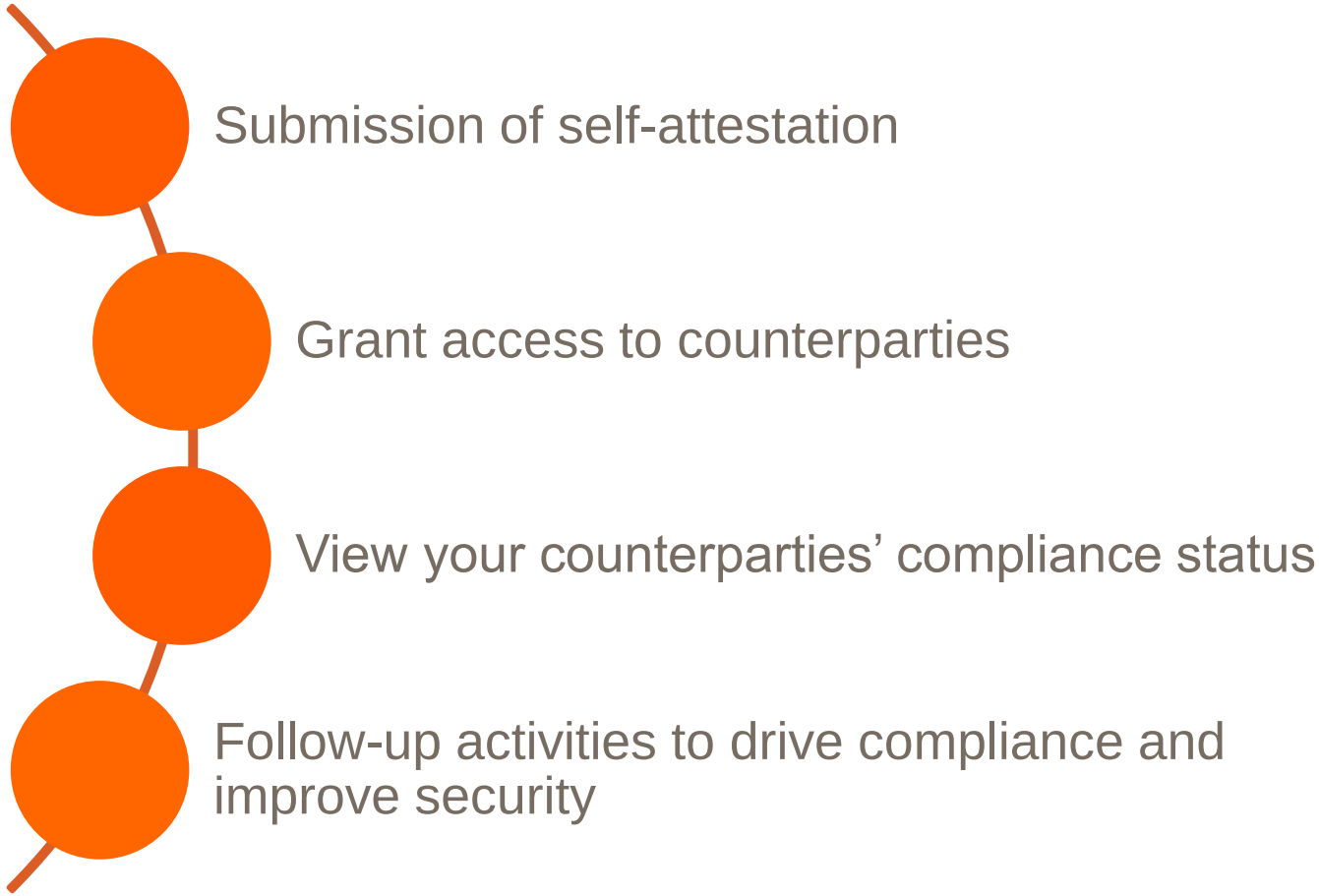
- To share compliance results with counterparties, as deemed appropriate.
- Creates transparency and allows risk management and business decision-making

Open for data submission and consumption from July 2017

- You will need to renew or reconfirm your self attestation on at least an annual basis

CSP | You > Security Guidelines and Assurance

Attestation



CSP | You > Security Guidelines and Assurance
Attestation Content

Submitter and approver info

Evaluation method (self-assessment, internal audit, external audit)

Type of infrastructure (including hub owner or service bureau if applicable)

Contact information

For each control:

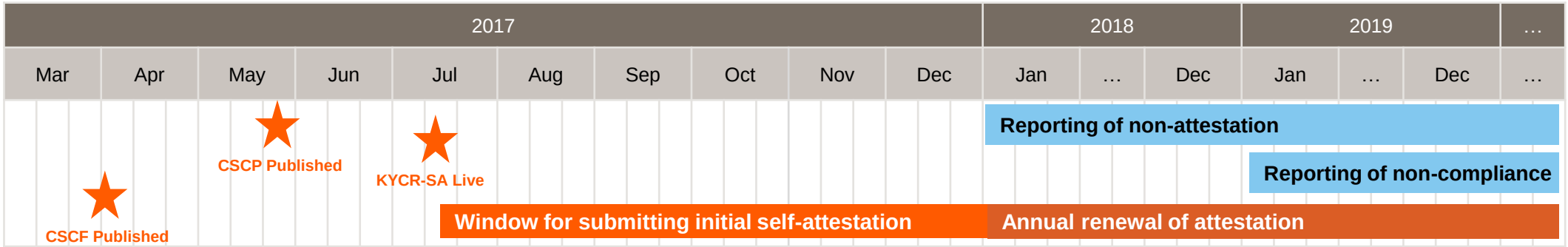
- ❑ I comply
  - → in line with guidance
  - → with alternative implementation
- ❑ I will comply
  - → with qualification date field
- ❑ I do not comply

Any mandatory control with a missing response will default to “Do not comply”

Advisory controls may be left with a blank response

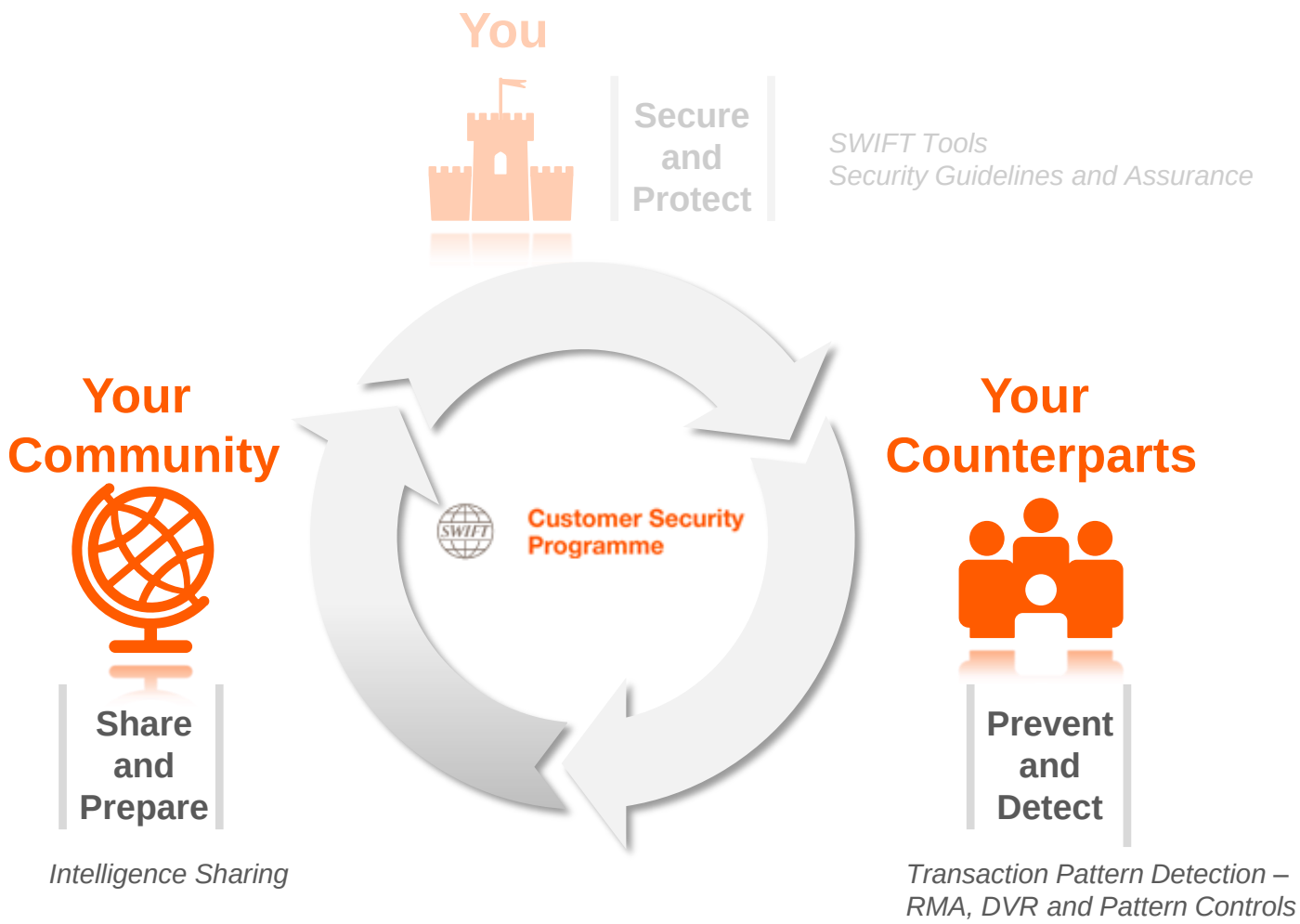
CSP | You > Security Guidelines and Assurance

Timeline Summary



- 31st March, 2017: Publication of SWIFT Customer Security Controls Framework
- 22nd May, 2017: Publication of SWIFT Customer Security Controls Policy
- July 2017, KYC Registry Security Attestation application available for data submission and consumption
- **As of end December 2017, all users must have submitted their self-attestation**
- As of Jan, 2018: SWIFT reserves the right to report users that have not submitted a self-attestation
- As of Jan, 2019: SWIFT reserves the right to report non-attested users and non-compliance

CSP | Programme
Beyond Securing and Protecting



CSP | Your Counterparts

Relationship Management Application - RMA

RMA and RMA plus

Poor management of RMAs creates potential security risks

Wolfsberg principles suggest that risks of RMA should be assessed. Approvals should be controlled and segregated between customer relationships and non-customers, with distinct due diligence criteria for each. Due diligence should consider the scope of message types used.

Only 40% of RMA relationships are actively used

Unilateral RMA revocation is now easy and is confirmed within 15 minutes

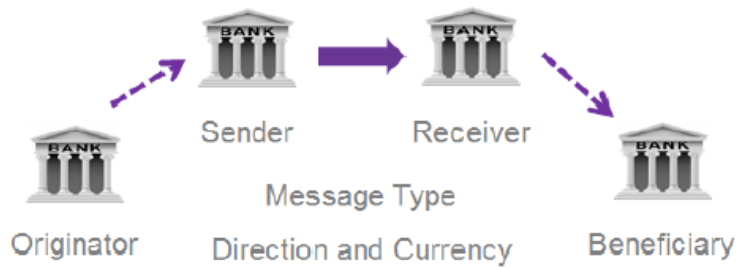
"RMA and RMA Plus: managing your correspondent connections" **info-paper provides details on best practice**

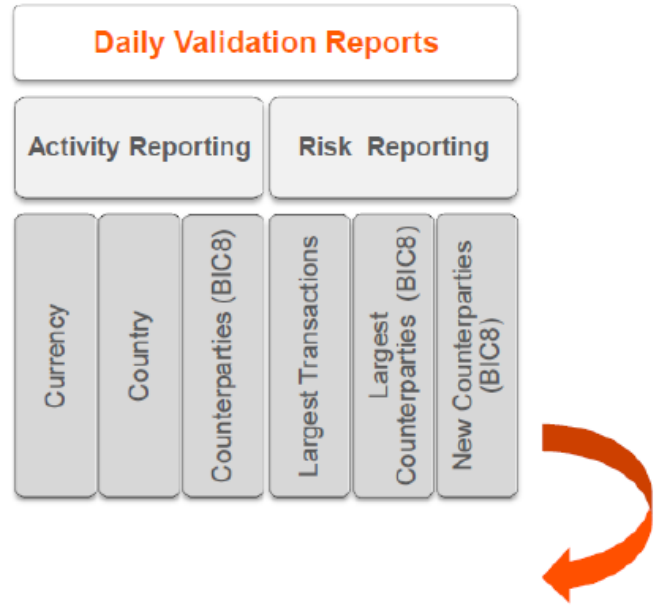
CSP | Your Counterparts
Transaction Pattern Detection - DVR

Daily Validation Reports

Activity Reporting – reports aggregate daily activity by message type, currency, country and counterparties with daily volume and value totals, maximum value of single transactions and comparisons to daily volume and value averages

Risk Reporting - highlights large or unusual message flows based on ordered lists for largest single transactions and largest aggregate transactions for counterparties, and a report on new combinations of counterparties to identify new relationships





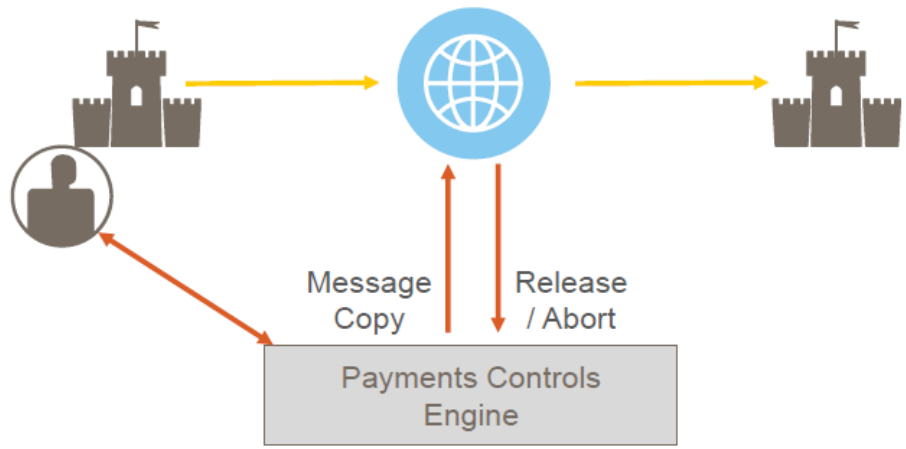
New Counterparties Reporting -
highlights any new combinations of direct and indirect counterparties. Makes it easy to identify new payment relationships that may be indicative of risk, and helps you quickly understand the values and volumes of the transactions involved

CSP | Your Counterparts
Payment Controls

Payment Controls

SWIFT is developing Payment Controls for subscribing organisations, performing 'in-flight' transaction monitoring **to identify payment activity that is out-of-policy or indicative of fraud risks**.

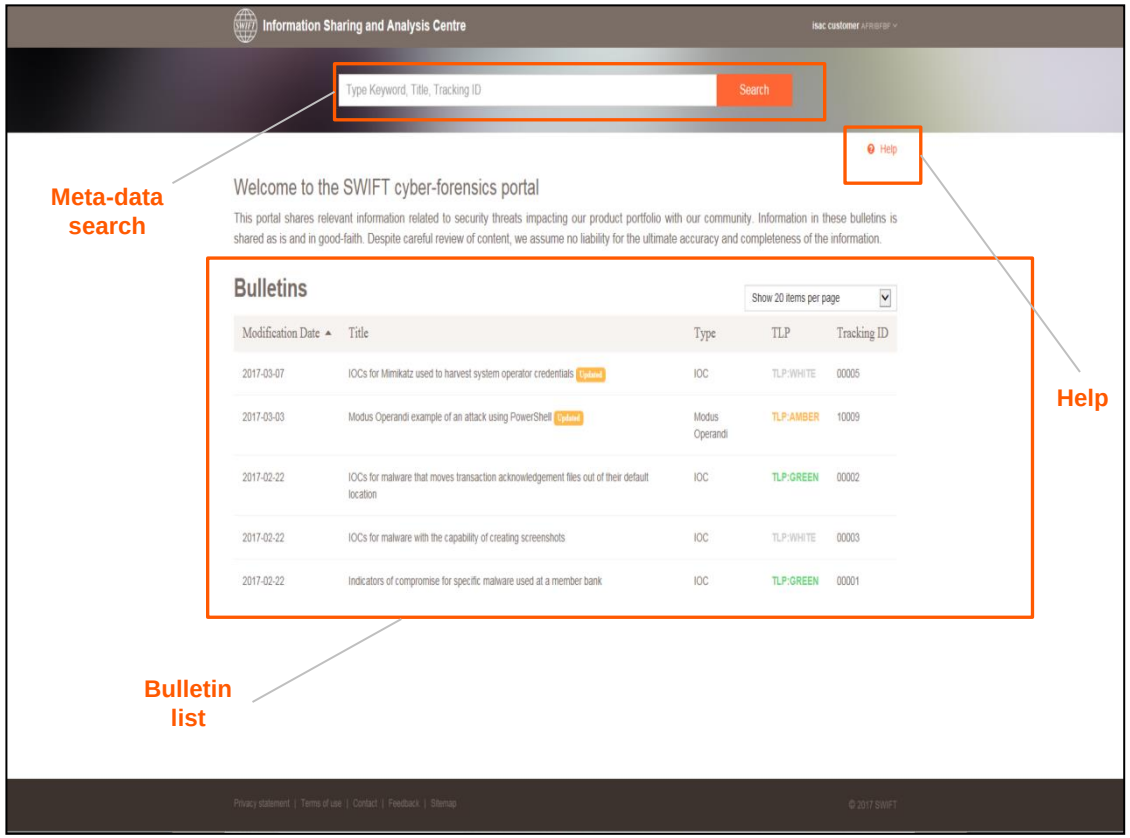
Payments Controls provide an additional safeguard on top of users' existing fraud prevention systems.

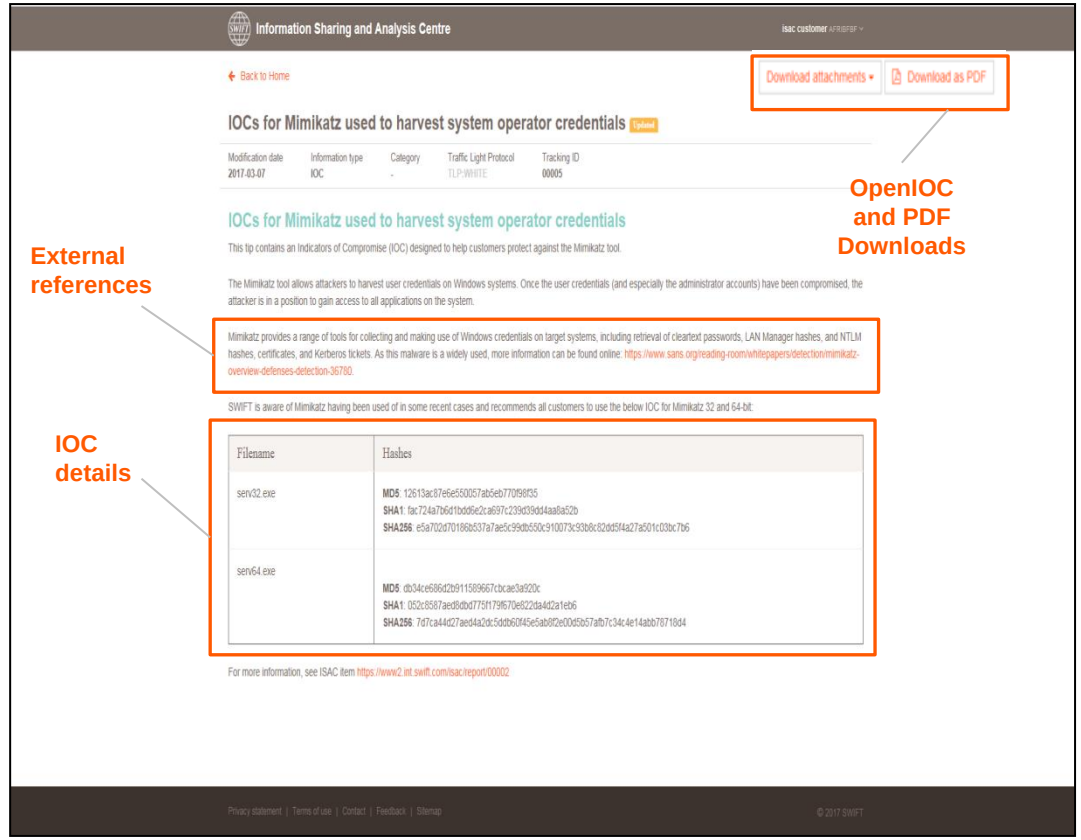


Focus on Smaller Institutions
Initially for smaller, sending organisations.
Will also help protect larger organisations through reduced risks of received payments.

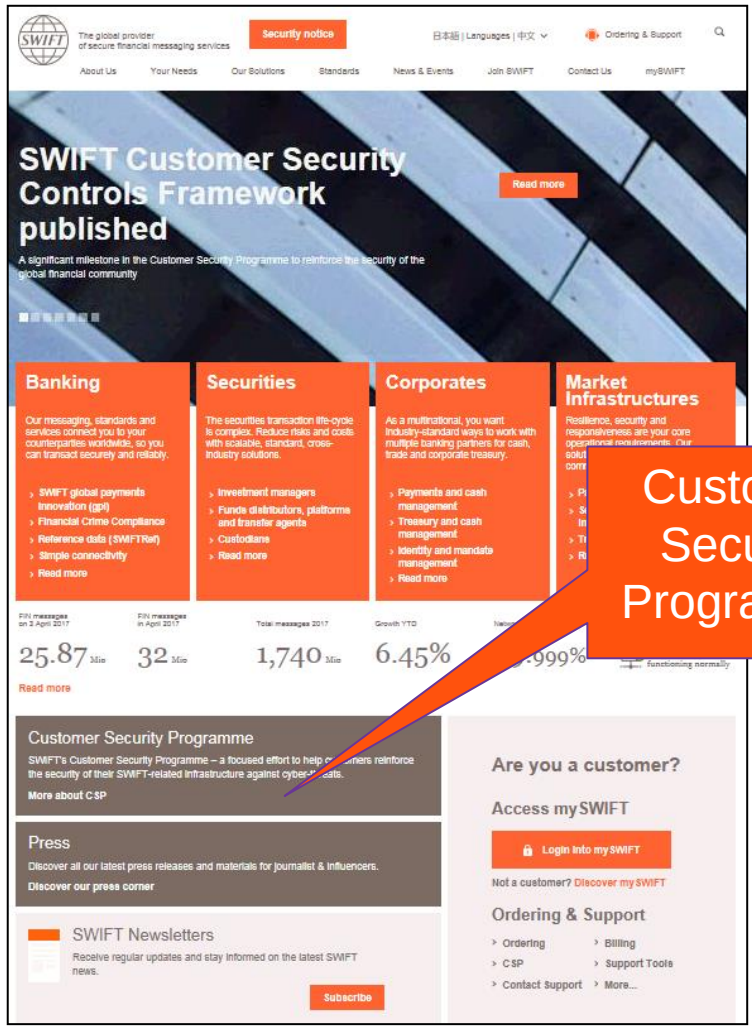
Secure In-Network
Using sanctions screening model to alert/release/abort payment messages in real-time. Monitoring policy defined by the subscriber.

CSP | Your Community
Intelligence Sharing: SWIFT-ISAC

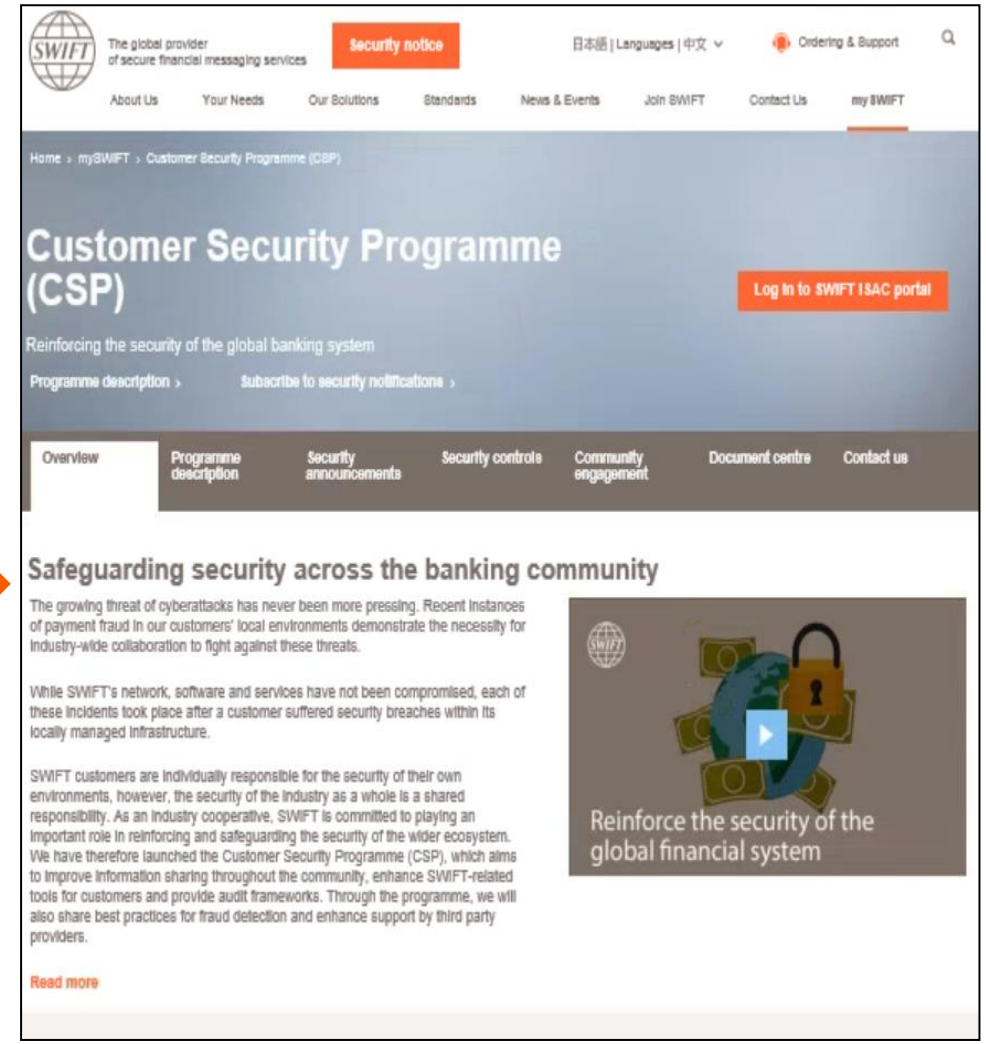




CSP | SWIFT.com



Customer Security Programme



Feedback, questions and open discussion

www.swift.com