



# 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

**30.4 million**

FIN messages peak day (2016)

**6.5+ billion**

FIN messages per year (2016)

**6.5%**

Increase in FIN traffic (2016)

**11,000+**

SWIFT users

**200+**

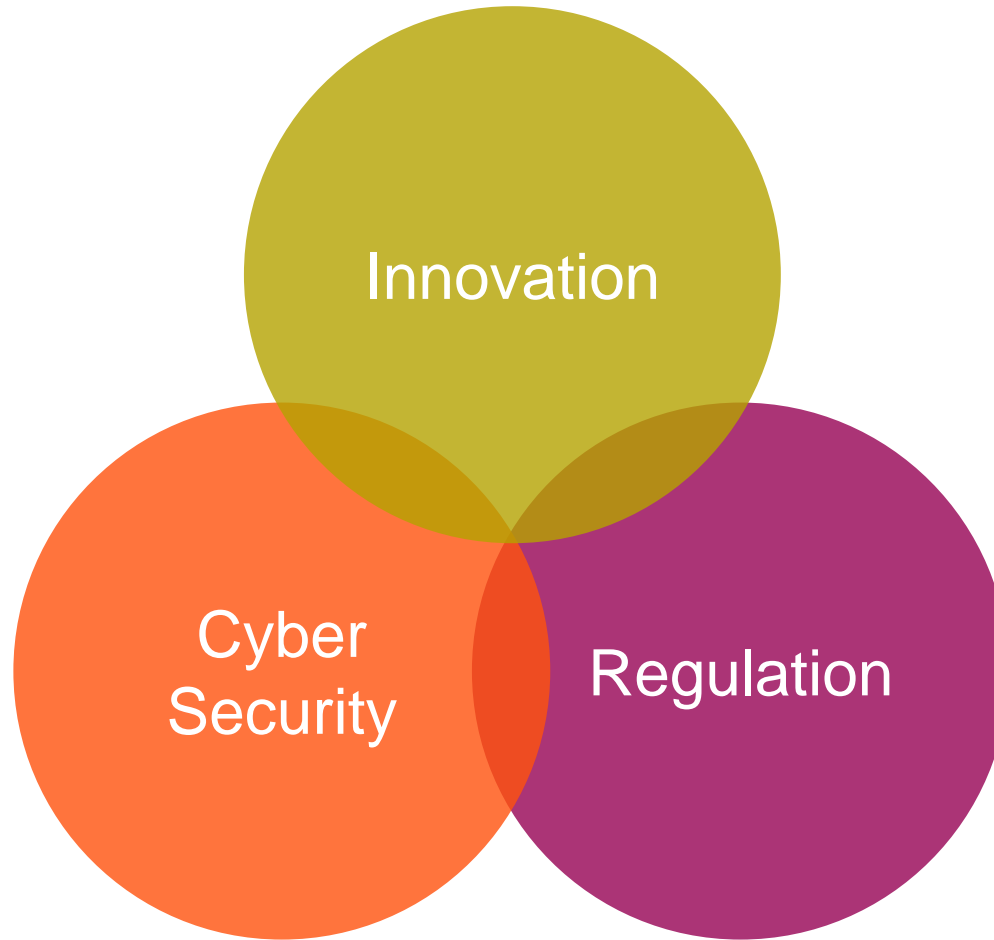
Countries and territories



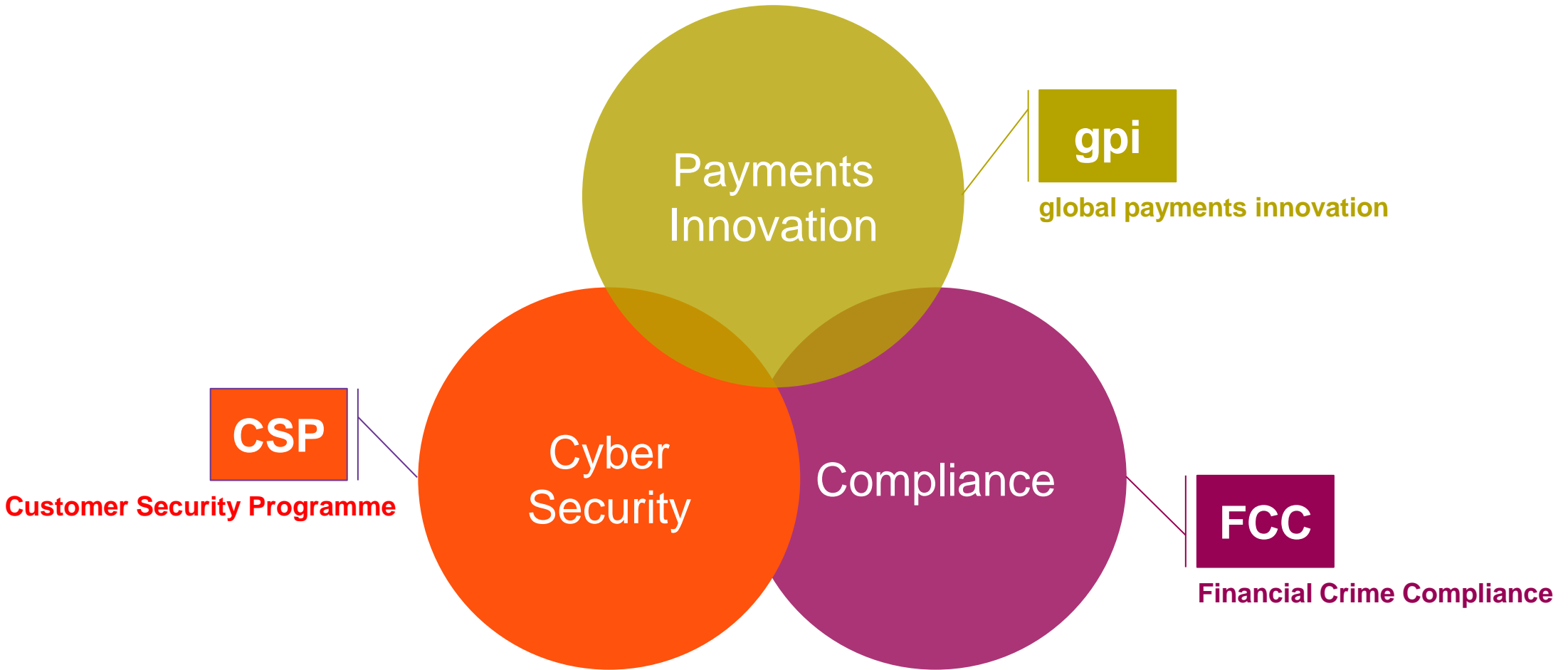


# Industry Change & Challenges

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



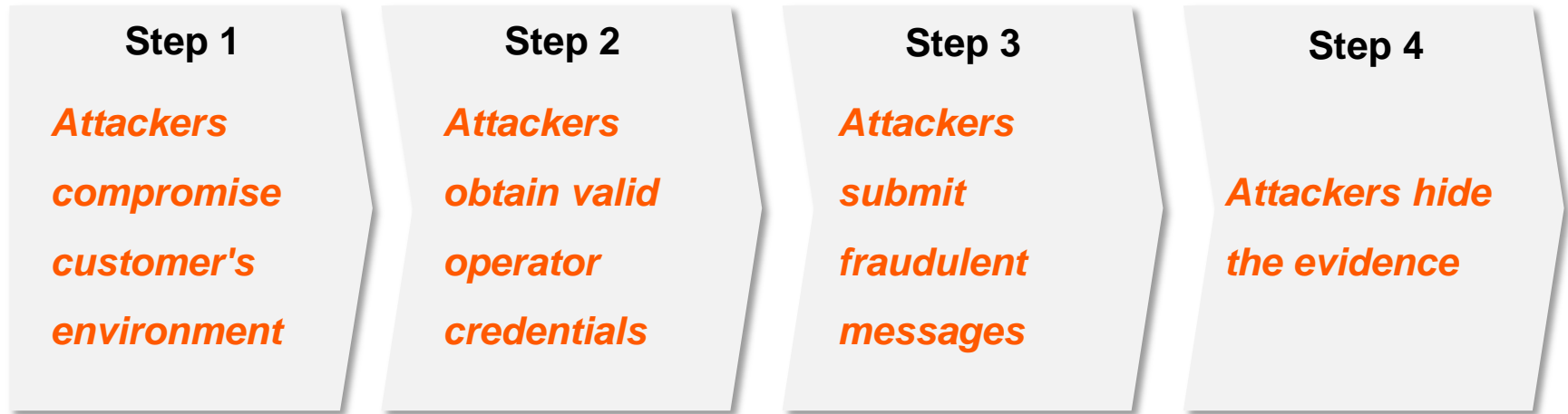
SWIFT is leading 3 initiatives, that combined take correspondent banking to the next level





# Customer Security Programme (CSP)

## CSP | Modus Operandi



- 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



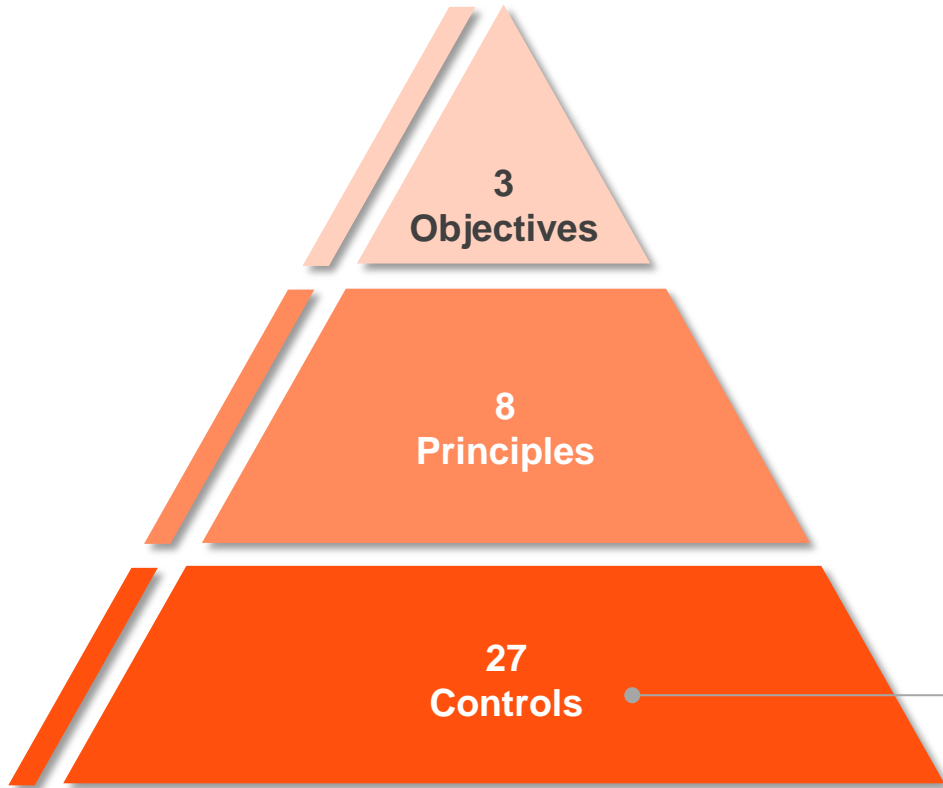
*Launched on May 27th 2016, CSP supports all customer segments, whether directly or indirectly connected, in reinforcing the security of their SWIFT-related infrastructure*





# 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

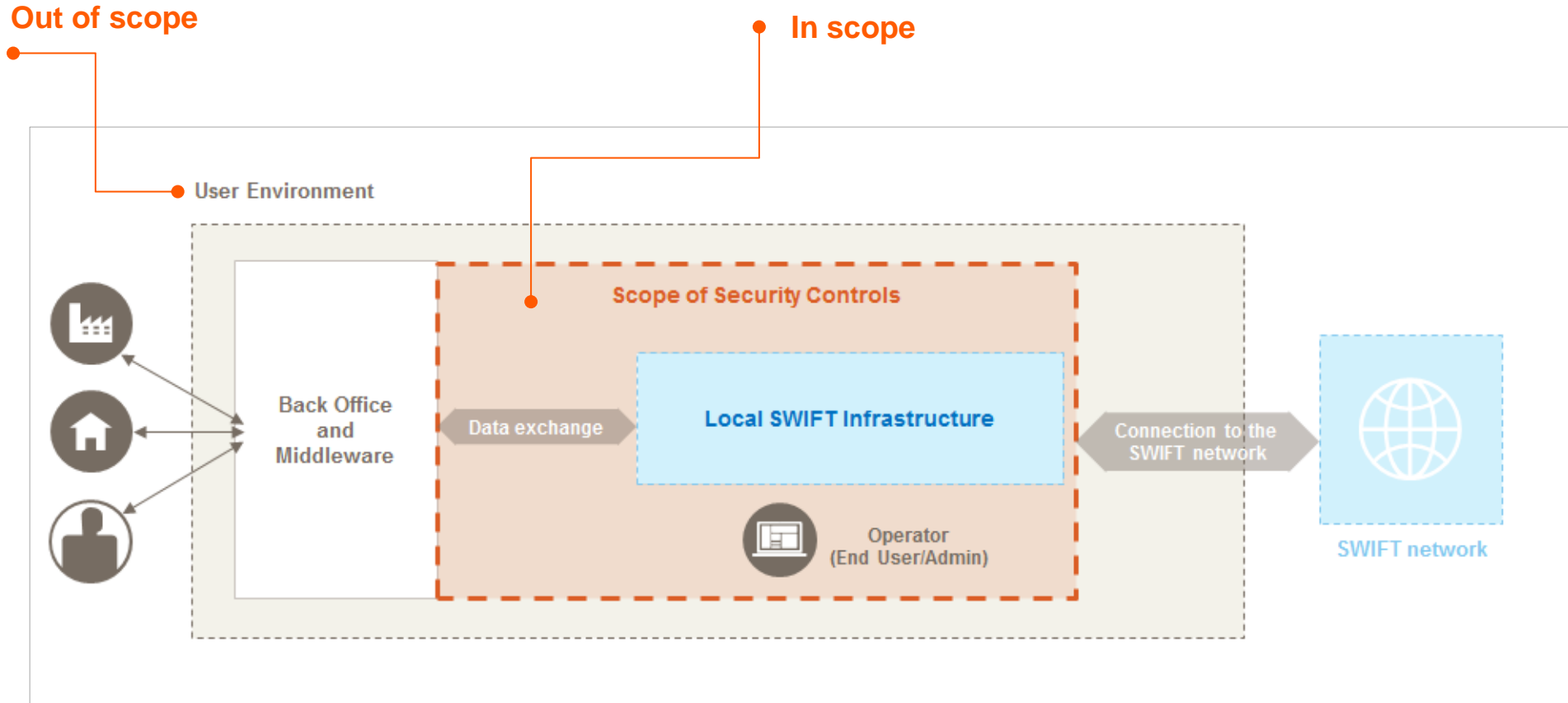
7. Detect anomalous activity to system or transaction records
8. Plan for incident response and information sharing

- *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*



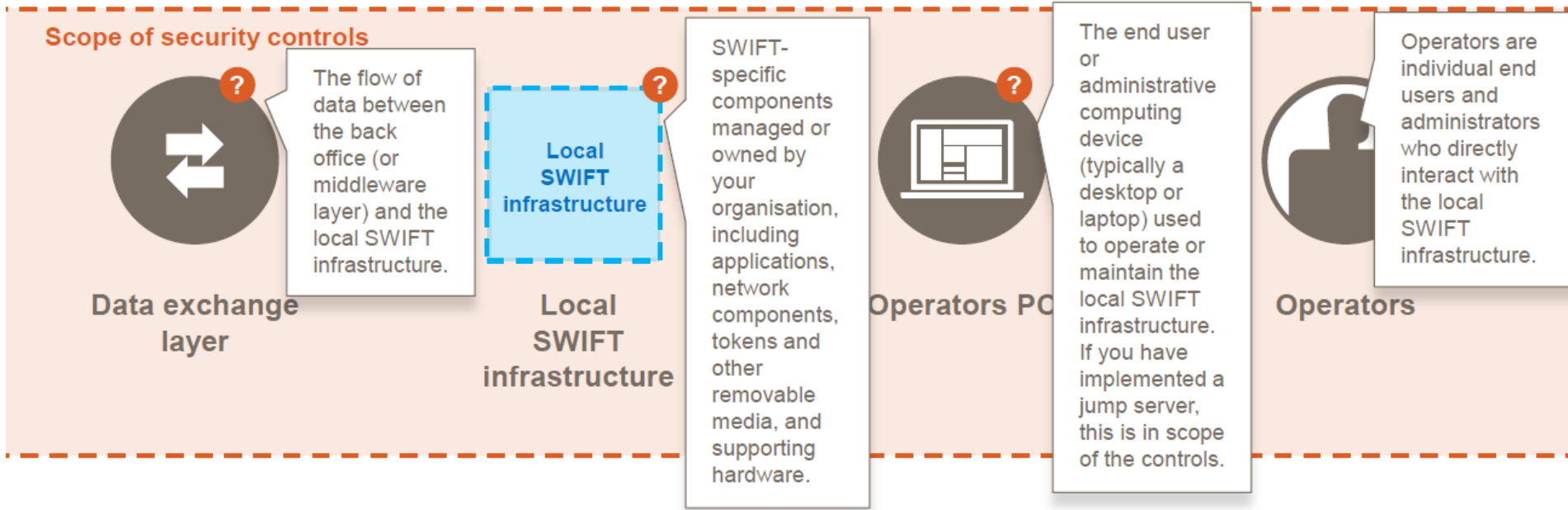
# CSP | You > Security Guidelines and Assurance

## 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>

---

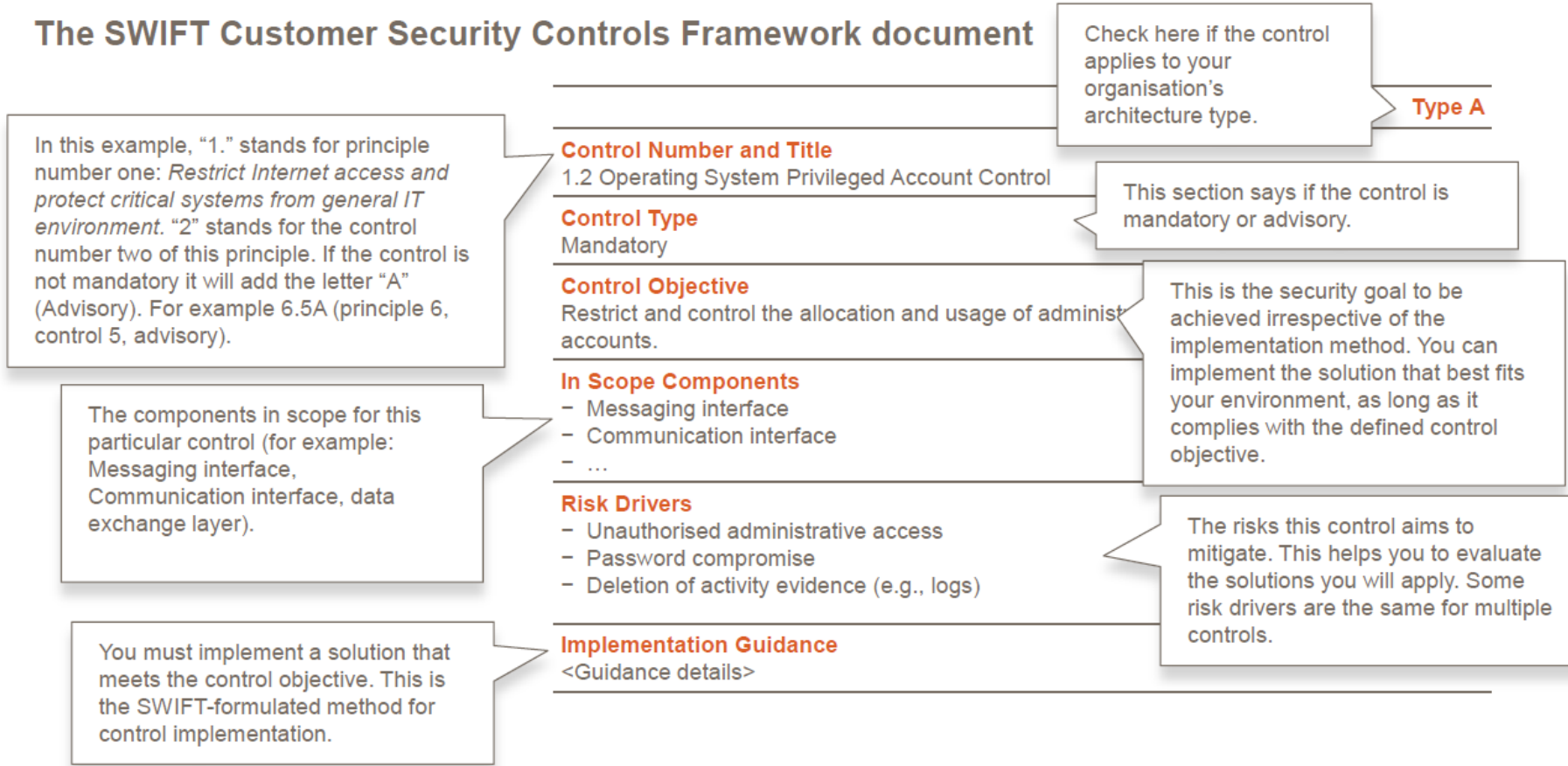




# CSP | You > Security Guidelines and Assurance

## Controls Framework

### The SWIFT Customer Security Controls Framework document





# CSP | You > Security Guidelines and Assurance Controls

Mandatory and Advisory Security Controls	A	B
<b>1 Restrict Internet Access and Protect Critical Systems from General IT Environment</b>		
1.1 SWIFT Environment Protection	•	
1.2 Operating System Privileged Account Control	•	
<b>2 Reduce Attack Surface and Vulnerabilities</b>		
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	•	•
<b>3 Physically Secure the Environment</b>		
3.1 Physical Security	•	•
<b>4 Prevent Compromise of Credentials</b>		
4.1 Password Policy	•	•
4.2 Multi-factor Authentication	•	•

Mandatory and Advisory Security Controls	A	B
<b>5 Manage Identities and Segregate Privileges</b>		
5.1 Logical Access Control	•	•
5.2 Token Management	•	•
5.3A Personnel Vetting Process	•	•
5.4A Physical and Logical Password Storage	•	•
<b>6 Detect Anomalous Activity to Systems or Transaction Records</b>		
6.1 Malware Protection	•	•
6.2 Software Integrity	•	
6.3 Database Integrity	•	
6.4 Logging and Monitoring	•	•
6.5A Intrusion Detection	•	
<b>7 Plan for Incident Response and Information Sharing</b>		
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](https://www.swift.com/CSP)



### Directory of cyber security service providers

Please find below the current directory of cyber security service providers, listing providers by the regions and countries in which they are currently operating.

#### Africa

Provider	Countries Covered
Provider A	South Africa
Provider information: Contact: Jane Doe Mail: Jane.Doe@Provider.com Phone: +01 (0) 23 45 67 89 Website: www.provider.com	
Provider B	Angola; South Africa
Provider C	South Africa

#### America North

Provider	Countries Covered
----------	-------------------

#### America South

Provider	Countries Covered
----------	-------------------

#### Asia Pacific

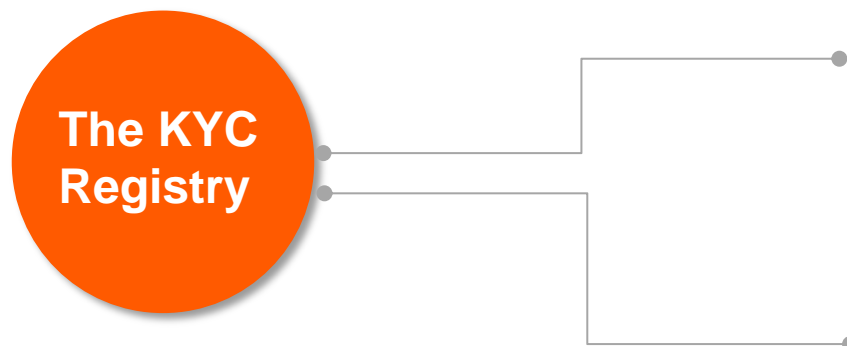
Provider	Countries Covered
----------	-------------------



## 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

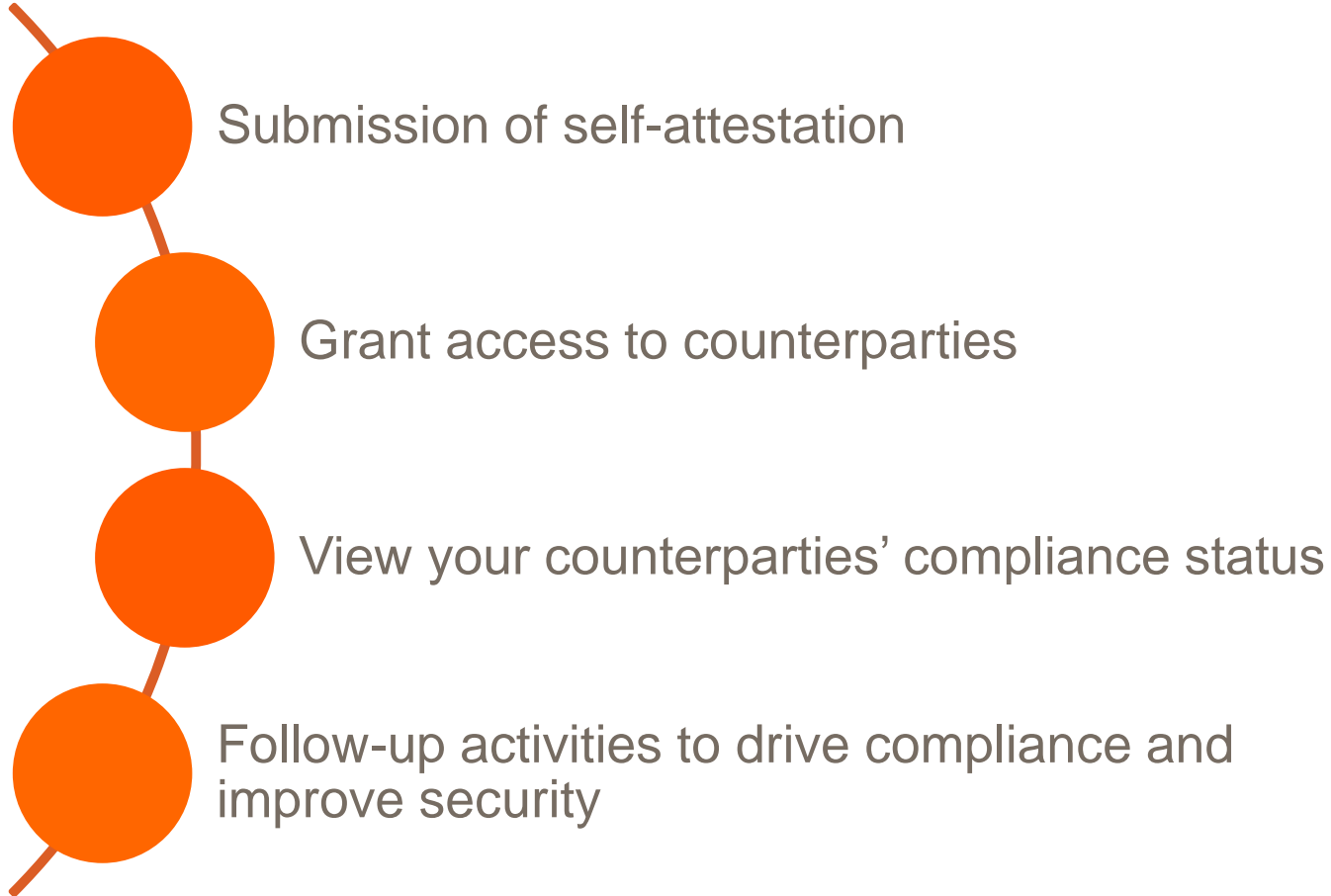
### **Open for data submission and consumption from July 2017**

- 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

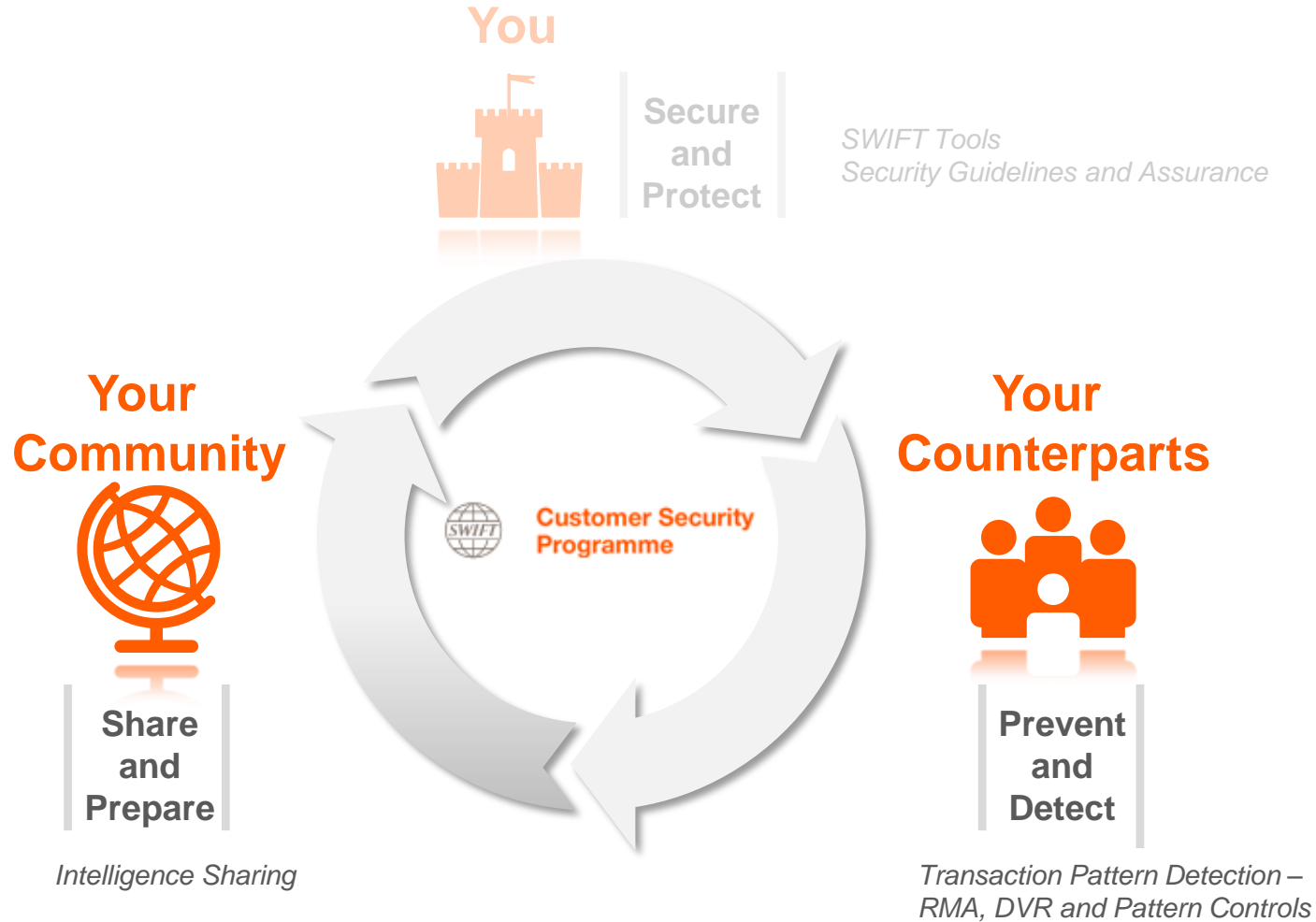






# CSP | Programme

*Beyond Securing and Protecting*





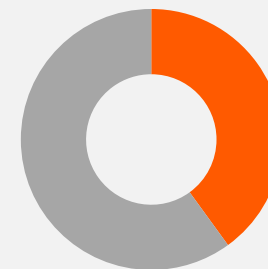
## CSP | Your Counterparts

### *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**



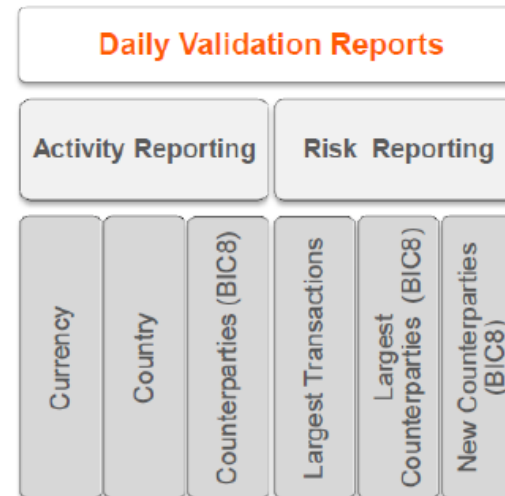
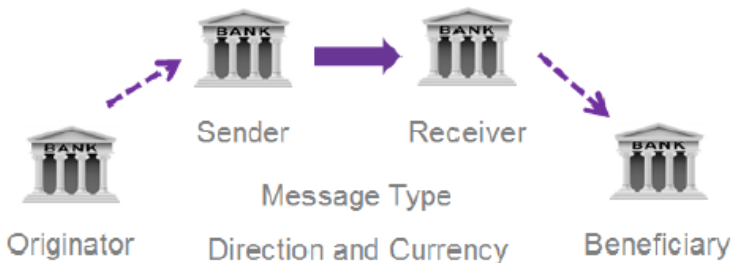
# CSP | Your Counterparts

## 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



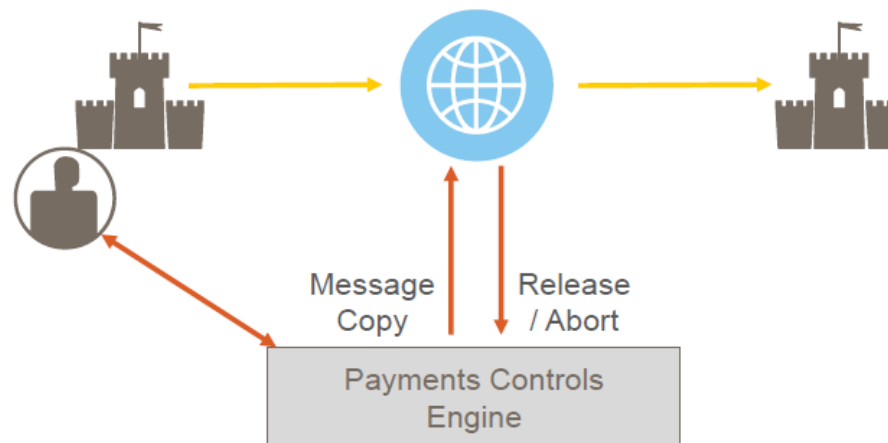
# CSP | Your Counterparts

## 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

**Meta-data search** (points to search bar)

**Help** (points to help icon)

**Bulletin list** (points to the table of bulletins)

**Help** (points to the main content area)

Information Sharing and Analysis Centre  
 Type Keyword, Title, Tracking ID Search  
 Welcome to the SWIFT cyber-forensics portal  
 This portal shares relevant information related to security threats impacting our product portfolio with our community. Information in these bulletins is shared as is and in good-faith. Despite careful review of content, we assume no liability for the ultimate accuracy and completeness of the information.

Modification Date	Title	Type	TLP	Tracking ID
2017-03-07	IOCs for Mimikatz used to harvest system operator credentials <b>Updated</b>	IOC	TLP-WHITE	00005
2017-03-03	Modus Operandi example of an attack using PowerShell <b>Updated</b>	Modus Operandi	TLP-AMBER	10009
2017-02-22	IOCs for malware that moves transaction acknowledgement files out of their default location	IOC	TLP-GREEN	00002
2017-02-22	IOCs for malware with the capability of creating screenshots	IOC	TLP-WHITE	00003
2017-02-22	Indicators of compromise for specific malware used at a member bank	IOC	TLP-GREEN	00001

© 2017 SWIFT

**External references** (points to the external references text)

**IOC details** (points to the file hashes table)

**OpenIOC and PDF Downloads** (points to download buttons)

Information Sharing and Analysis Centre  
 Back to Home  
 Download attachments Download as PDF  
 IOCs for Mimikatz used to harvest system operator credentials **Updated**

Modification date	Information type	Category	Traffic Light Protocol	Tracking ID
2017-03-07	IOC	-	TLP-WHITE	00005

**IOCs for Mimikatz used to harvest system operator credentials**

This tip contains an Indicator of Compromise (IOC) designed to help customers protect against the Mimikatz tool.

The Mimikatz tool allows attackers to harvest user credentials on Windows systems. Once the user credentials (and especially the administrator accounts) have been compromised, the attacker is in a position to gain access to all applications on the system.

Mimikatz provides a range of tools for collecting and making use of Windows credentials on target systems, including retrieval of cleartext passwords, LAN Manager hashes, and NTLM hashes, certificates, and Kerberos tickets. As this malware is a widely used, more information can be found online: <https://www.sans.org/reading-room/whitepapers/detection/mimikatz-overview-defenses-detection-36780>.

SWIFT is aware of Mimikatz having been used of in some recent cases and recommends all customers to use the below IOC for Mimikatz 32 and 64-bit.

Filename	Hashes
serv32.exe	MD5: 12613ac87e6e55007ab56b77098f35 SHA1: f0c724b76d1bd9e2ca697c239d39d4aa6a572b SHA256: e5a702d70186b537a7aefc99db500c910079c93b6832d95f4427a501c03bc7b6
serv64.exe	MD5: db34ce68d29911589667cbca3a920c SHA1: 052c8587aeb3dbd7731739670e8209442a1eb6 SHA256: 7d7ca4427ae44a20c545bb6045e5ab92e005957ab7c34c4e14abb7871804

For more information, see ISAC Item <https://www2.int.swift.com/isac/report/00002>

© 2017 SWIFT





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

# SWIFT Customer Security Controls Framework published

A significant milestone in the Customer Security Programme to reinforce the security of the global financial community

[Read more](#)

**Banking**

Our messaging, standards and services connect you to your counterparties worldwide, so you can transact securely and reliably.

- > SWIFT global payments Innovation (gpi)
- > Financial Crime Compliance
- > Reference data (SWIFTRail)
- > Simple connectivity
- > Read more

**Securities**

The securities transaction life-cycle is complex. Reduce risks and costs with scalable, standard, cross-industry solutions.

- > Investment managers
- > Funds distributors, platforms and transfer agents
- > Custodians
- > Read more

**Corporates**

As a multinational, you want industry-standard ways to work with multiple banking partners for cash, trade and corporate treasury.

- > Payments and cash management
- > Treasury and cash management
- > Identity and mandate management
- > Read more

**Market Infrastructures**

Resilience, security and responsiveness are your core operational requirements. Our global core

- > PI
- > SI
- > TI
- > RI

EN messages on 2 April 2017: 25.87 36m

EN messages on 4 April 2017: 32 36m

Total messages 2017: 1,740 36m

Growth YTD: 6.45%

functioning normally

[Read more](#)

**Customer Security Programme**

SWIFT's Customer Security Programme – a focused effort to help customers reinforce the security of their SWIFT-related infrastructure against cyber threats.

[More about CSP](#)

**Press**

Discover all our latest press releases and materials for journalist & influencers.

[Discover our press corner](#)

**SWIFT Newsletters**

Receive regular updates and stay informed on the latest SWIFT news.

[Subscribe](#)

**Are you a customer?**

[Access mySWIFT](#)

[Login into mySWIFT](#)

Not a customer? [Discover mySWIFT](#)

**Ordering & Support**

- > Ordering
- > Billing
- > CSP
- > Support Tools
- > Contact support
- > More...

Customer Security Programme



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

[Log in to SWIFT ISAC portal](#)

Programme description > [Subscribe to security notifications >](#)

Overview Programme description Security announcements Security controls Community engagement Document centre Contact us

## Safeguarding security across the banking community

The growing threat of cyberattacks has never been more pressing. Recent instances of payment fraud in our customers' local environments demonstrate the necessity for industry-wide collaboration to fight against these threats.

While SWIFT's network, software and services have not been compromised, each of these incidents took place after a customer suffered security breaches within its locally managed infrastructure.

SWIFT customers are individually responsible for the security of their own environments, however, the security of the industry as a whole is a shared responsibility. As an industry cooperative, SWIFT is committed to playing an important role in reinforcing and safeguarding the security of the wider ecosystem. We have therefore launched the Customer Security Programme (CSP), which aims to improve information sharing throughout the community, enhance SWIFT-related tools for customers and provide audit frameworks. Through the programme, we will also share best practices for fraud detection and enhance support by third party providers.

[Read more](#)

**Reinforce the security of the global financial system**





Feedback,  
questions and  
open discussion



[www.swift.com](http://www.swift.com)