Operations Forum 2021

SWIFT Customer Security Programme
Managing the evolving cyber threat

Olivier Dazard
Head of Control Frameworks Programme
Strategy & Engagement
SWIFT

Frank Versmessen
Manager, Customer Security
SWIFT

Ruth Montgomery
Lead Security Management Specialist
SWIFT

Sofie Vuylsteke
Lead Security Management Specialist
SWIFT

Customer Security Programme | Value

Cybercriminals relentlessly target financial institutions and large corporations to **steal assets**

Banks and custodians safeguard their customers' assets

CSP is designed to **help** dealing with cybercrime and protecting against asset theft

Know-how

Attacks

Controls

Risk Mgmt

Customer Security Programme | Compliance Evolution

CSCF v2017
27 Controls
Jan 2018

77% Average
Compliance Rate
Across All Controls
(52%-88% Range)

Mandated Compliance

CSCF v2018
27 Controls
Jan 2019

94% Average
Compliance Rate
Across All Controls
(86%-97% Range)

Added 2 New Controls
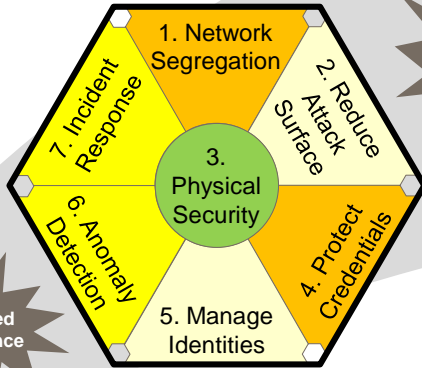
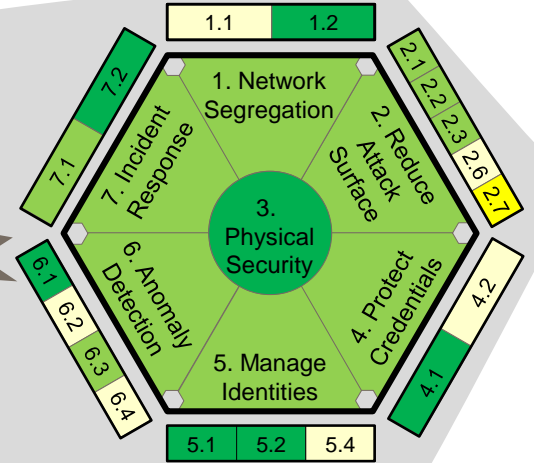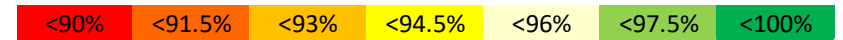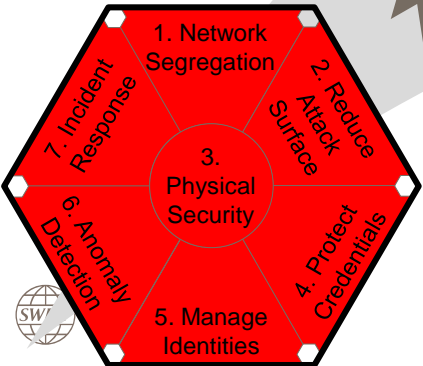**CSCF v2019**
29 Controls
Jan 2020

96% Average
Compliance Rate
Across All Controls
(89%-98% Range)
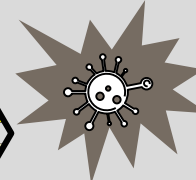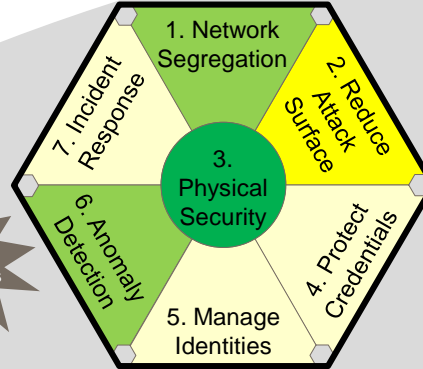
CSCF v2019
29 Controls
Jan 2021

97% Average
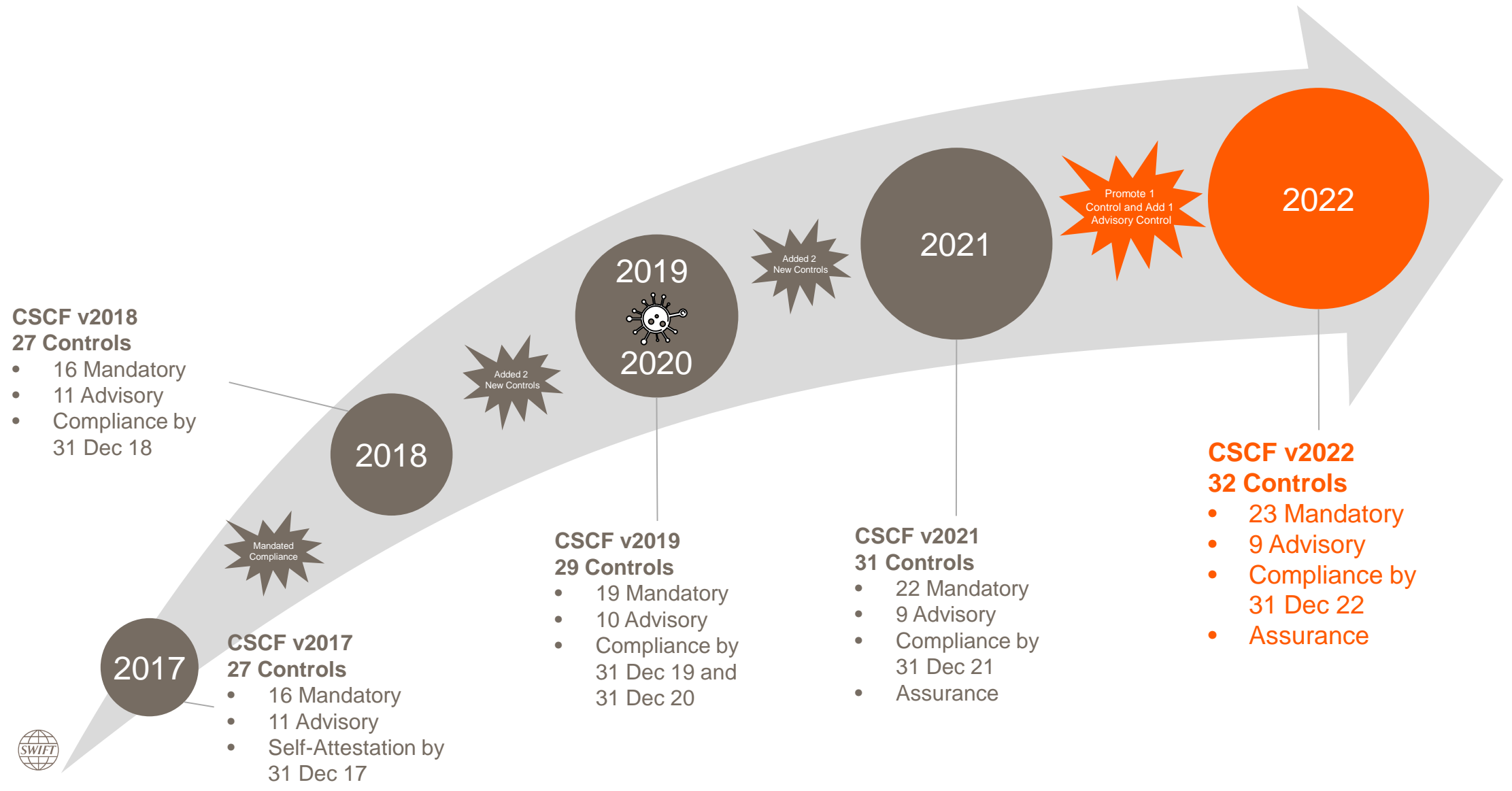Compliance Rate
Across All Controls
(93%-99% Range)

Hexagon segments (each version): 1. Network Segregation, 2. Reduce Attack Surface, 3. Physical Security, 4. Protect Credentials, 5. Manage Identities, 6. Anomaly Detection, 7. Incident Response

Control sub-items (Jan 2021): 1.1, 1.2, 2.1, 2.2, 2.3, 2.6, 2.7, 4.1, 4.2, 5.1, 5.2, 5.4, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2

Legend: <90% | <91.5% | <93% | <94.5% | <96% | <97.5% | <100%

Customer Security Programme
CSCF and IAF in 2021 and beyond

CSCF Controls | Evolution since 2017

SWIFT **Customer Security Programme**

2022

2021

Promote 1 Control and Add 1 Advisory Control

2019
2020

Added 2 New Controls

2018

Added 2 New Controls

Mandated Compliance

2017

SWIFT

CSCF v2018
27 Controls
- 16 Mandatory
- 11 Advisory
- Compliance by 31 Dec 18

CSCF v2017
27 Controls
- 16 Mandatory
- 11 Advisory
- Self-Attestation by 31 Dec 17

CSCF v2019
29 Controls
- 19 Mandatory
- 10 Advisory
- Compliance by 31 Dec 19 and 31 Dec 20

CSCF v2021
31 Controls
- 22 Mandatory
- 9 Advisory
- Compliance by 31 Dec 21
- Assurance

CSCF v2022
32 Controls
- 23 Mandatory
- 9 Advisory
- Compliance by 31 Dec 22
- Assurance

CSCF v2021 | Most important changes

Customer Security Programme

1. Introduced Architecture type A4 – **Customer Connector**

2. Fully transfer 'Internet Access' provisions from control 1.1 to 1.4 (Restrict Internet Access)

3. Extended definition of **General purpose operator PC**

4. Many clarifications throughout

Mandatory and Advisory Security Controls	A1	A2	A3	A4	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	•	•	•	•	
1.3 Virtualisation Platform Protection	•	•	•	•	
1.4 Restriction of Internet Access	•	•	•	•	•
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	•	•	•	•	•
2.6 Operator Session Confidentiality and Integrity	•	•	•	•	
2.7 Vulnerability Scanning	•	•	•	•	•
2.8A Critical Activity Outsourcing	•	•	•	•	•
2.9A Transaction Business Controls	•	•	•	•	•
2.10 Application Hardening	•	•	•	•	
2.11A RMA 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	•	•	•	•	
5 Manage Identities and Segregate Privileges					
5.1 Logical Access Control	•	•	•	•	•
5.2 Token Management	•	•	•	•	•
5.3A Personnel Vetting Process	•	•	•	•	•
5.4 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	•	•	•	•	•

CSCF Change Management Process | Consultation Timeline and WG Meetings

Kick-off information meetings

Processing feedback

"Nihil Obstat" & Board approval

Dec 2021 — Jan 2022 — Feb 2022 — Mar 2022 — Apr 2022 — May 2022 — Jun 2022 — Jul 2022

Mailing feedback form

Feedback form due date

Draft to SWIFT Oversight

CSCF v2023 publication

CSCF WG meetings (dates TBC)

Customer Security Programme
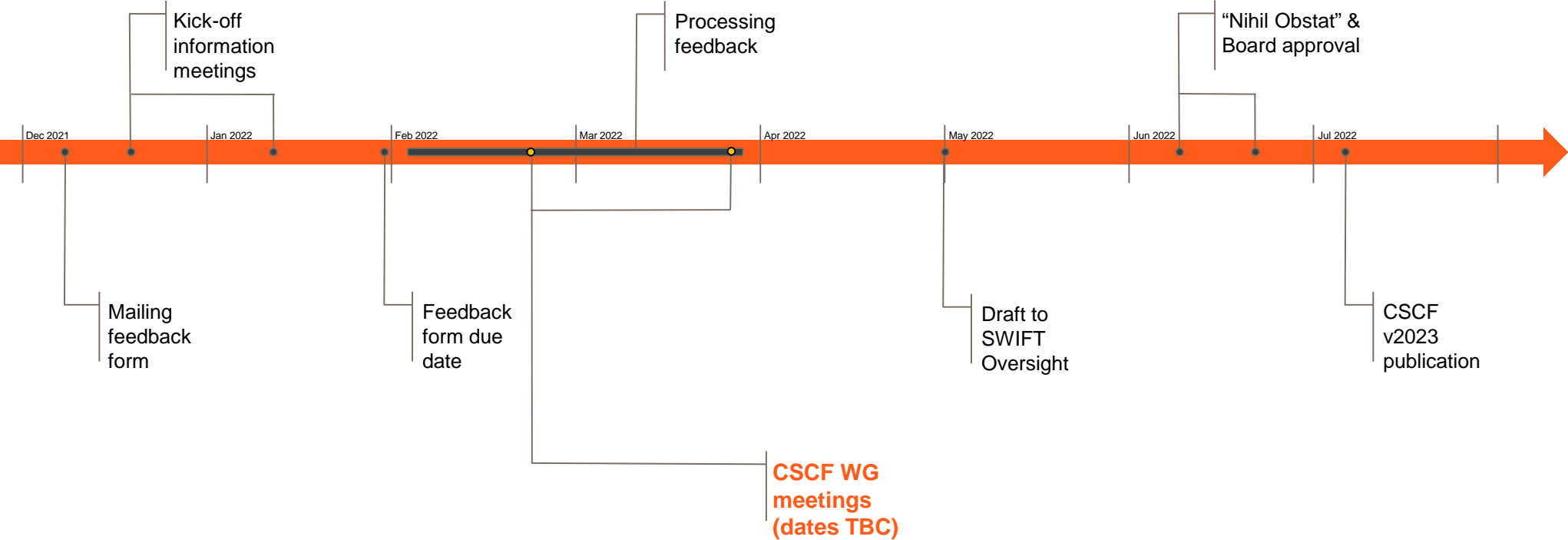
1 **Promotion of Control 2.9A** (Transaction Business Controls) **to 'mandatory'** after important scope and implementation guidelines clarifications

2 **New Advisory Control 1.5A** (Customer Environment Protection) to align requirements, of Architecture A4 with the other type 'A' Architectures

3 Change of Scope Impacting Numerous Controls for CSCF v2022:
- Extend the scope of all controls for **Architecture A4 to include** '**Customer Connector'** as an 'in scope' component
- Extend the scope of existing **Control 1.2** (Operating System Privileged Account Control) to include 'General Purpose Operator PCs' as 'advisory' to ensure basic security hygiene on employee computers
- Extend the scope of existing **Control 6.2** (Software Integrity) for Architecture A4 to include 'customer connectors' components as 'advisory'

4 **Minor but numerous Guidance Clarifications or Changes**

Customer Security Programme

- A mandatory **External and/or Internal Independent** assessment to confirm the compliance with mandatory controls

- Self-assessment still available but considered as not compliant

- **Clarifications** on assessors **certifications**

- **Eligibility** of service providers (under conditions) as assessment providers for their customers

- **Tested** curriculum required for assessment providers prior to their listing on swift.com

- **Additional and revised resources** for assessment providers:
  - New High Level test plan **guidance**
  - New Independent Assessment process **guidance**
  - Revised Assessment **templates**
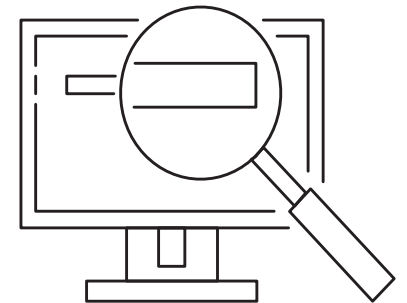
ebook: Unlocking the Value of Your Counterparties' CSP Attestation Data

- Sharing attestation data is an important tool in managing counterparty risk, and in 2021, **requests to share counterparty data have increased by over 45% - of which 28% were from first time senders** - indicating increased attention to this area

- New ebook *Unlocking the Value of Your Counterparties' CSP Attestation Data* shares insights from leading institutions on how to develop a counterparty risk management strategy
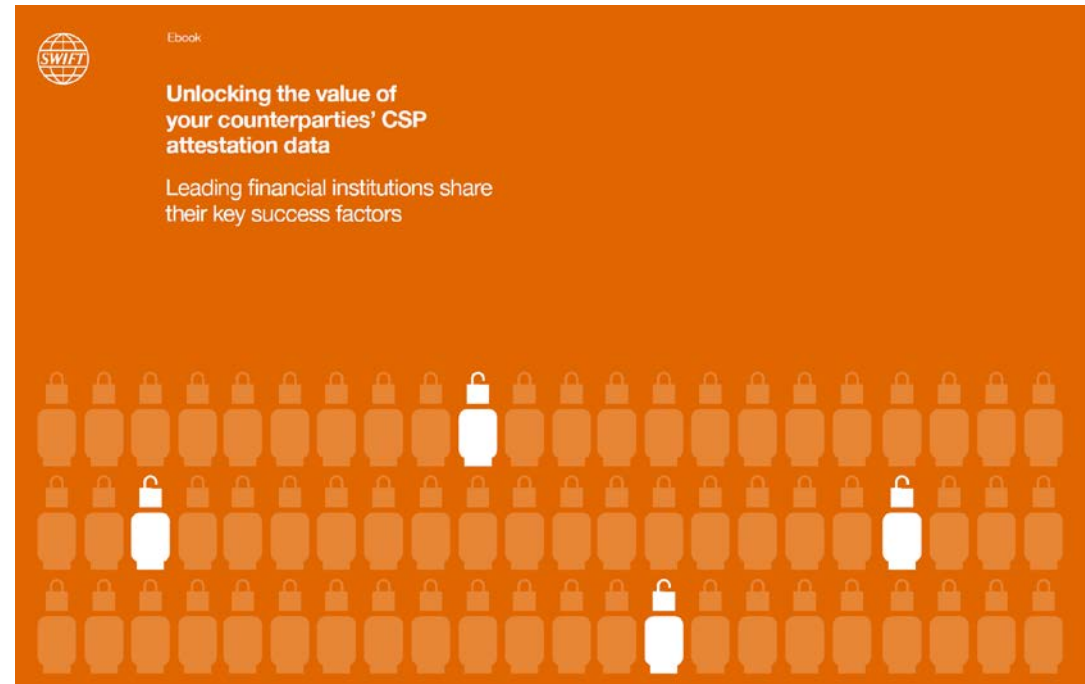
Six leading institutions which are early adopters in this area shared their experiences on developing counterparty risk management processes to manage attestation data

Getting more out of your CSP attestation data

CUSTOMER SECURITY PROGRAMME, 6 OCTOBER 2021 | 3 MIN READ

SIBOS panel discussion, available to view on demand at sibos.com until end of December:

▶ AVAILABLE ON DEMAND

Unlocking the value of CSP attestation data for counterparty risk management

Managing risk   SWIFT

Risk management is central to SWIFT's DNA. And for the SWIFT community operating with the ongoing threat of cyberattacks, the move to ISO 20022 and our enhanced platform brings an increased focus on data and counterparty risk management. SWIFT's Customer Security Programme continues moving the community towards ever ...

Read more ›

Cyber Security, Data

YOUR LOCAL TIME

12 OCT 11:00 › 11:30   REMOVE FROM MY LIST

SPEAKERS

Joanne Cash
THE BANK OF NEW
YORK MELLON

Leif Simon
DEUTSCHE BANK
AG

**Frank
Versmessen**
SWIFT

Access session →

The ebook aims to share examples of best practice which have enabled early adopters to develop an effective counterparty risk management strategy:

- Provides access to insights from institutions leading in this space

- How to improve cybersecurity in a way that is both affordable and accessible

- Features success factors which support process development

- Practical examples of areas for focus

- Key practical areas for focus:

  - Securing resources and engaging senior management
  - Communication planning with stakeholders
  - Developing tools to manage data
  - Engaging with counterparties and the community

- How and when to collect and assess counterparty data

- Handling counterparty non-compliance

- Planning and Execution Checklist

For the financial services ecosystem:

o Strengthens overall risk management processes

o Contributes to reinforcing the financial services ecosystem

For you and your messaging counterparties:

o Raises profile with counterparties

o Builds trust by demonstrating a clean bill of health

For your teams and stakeholders:

o Educates on CSP scope and its role in cybersecurity

o Extracts additional value from CSP attestation data

o Uses tools which are both affordable and accessible, and already available to your teams

Managing KYC-SA Counterparty Access Requests (ARs)

Managing Counterparty ARs | How-to

Requesting

- Ensure you have KYC-SA users with the requester role assigned (see tip 5021826)

- Requests can be sent **individually**, or up to 250 with one **bulk** access request

Checking

- Requesters, administrators and viewers can check the status of requests in the Data Access Requests Sent report, or the My Counterparties or My Messaging Counterparties screens

Viewing

- Requesters and viewers can view individual counterparty attestations

- KYC-SA security officers can download the My Counterparties Control Details report with attestation data of all counterparties which have given access

Managing Counterparty ARs | Individual request

Customer Security Programme

Managing Counterparty ARs | Bulk request

Managing Counterparty ARs | How to view

Customer Security Programme

Managing Counterparty ARs | How to request for Messaging Counterparties

- Two functions to make responding to access requests more efficient:

  - If opted in, **Grant All** processes access requests from Messaging Counterparties (status visible in My Messaging Counterparties, see tip 5024185)

  - Requests from BICs on the **Allow List** are automatically granted

- Ensure your institution has users with the granter role assigned, to respond to access requests (see tip 5021826)

- Notification of access requests received by your institution will appear in the granters' inbox

- Granters and administrators can check the status of all requests received in the Data Access Requests Received report

Demo of new features in KYC-SA

Customer Security Programme | Take Away

- Focus on the completion of your 2021 KYC-SA attestation and stay abreast of what is coming up in 2022

- Using counterparty attestation data will improve your cybersecurity risk management – to help you get started, leading early adopters have shared their experiences in the <u>new ebook</u> to point you in the right direction

- Use KYC-SA to check the compliance status of your entities and counterparties

www.swift.com