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

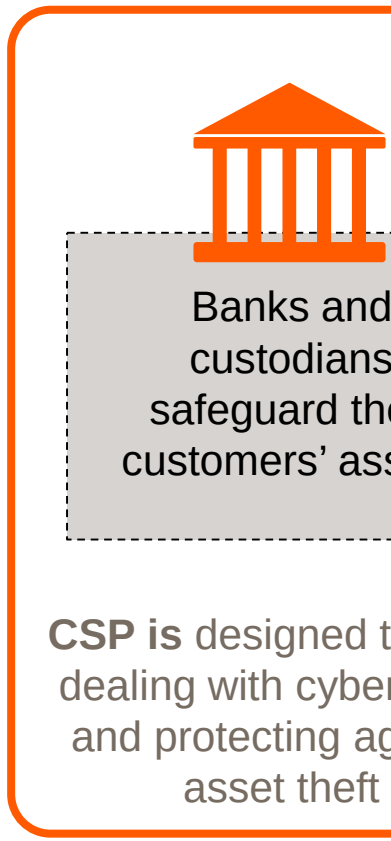
Ruth Montgomery
Lead Security Management Specialist
SWIFT

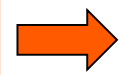
Sofie Vuylsteke
Lead Security Management Specialist
SWIFT

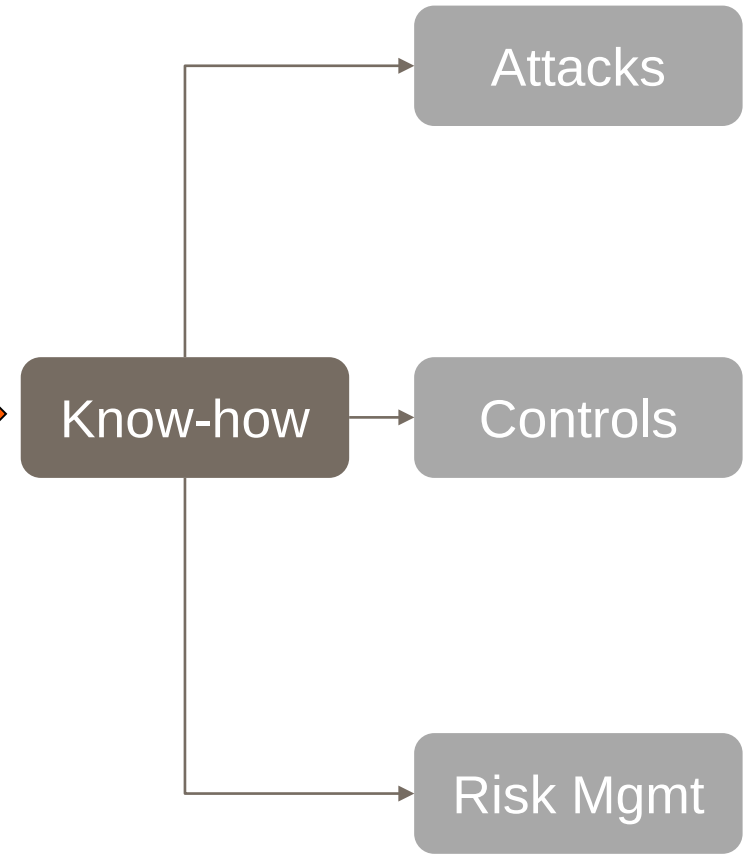
Customer Security Programme | Value

Customer Security Programme

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

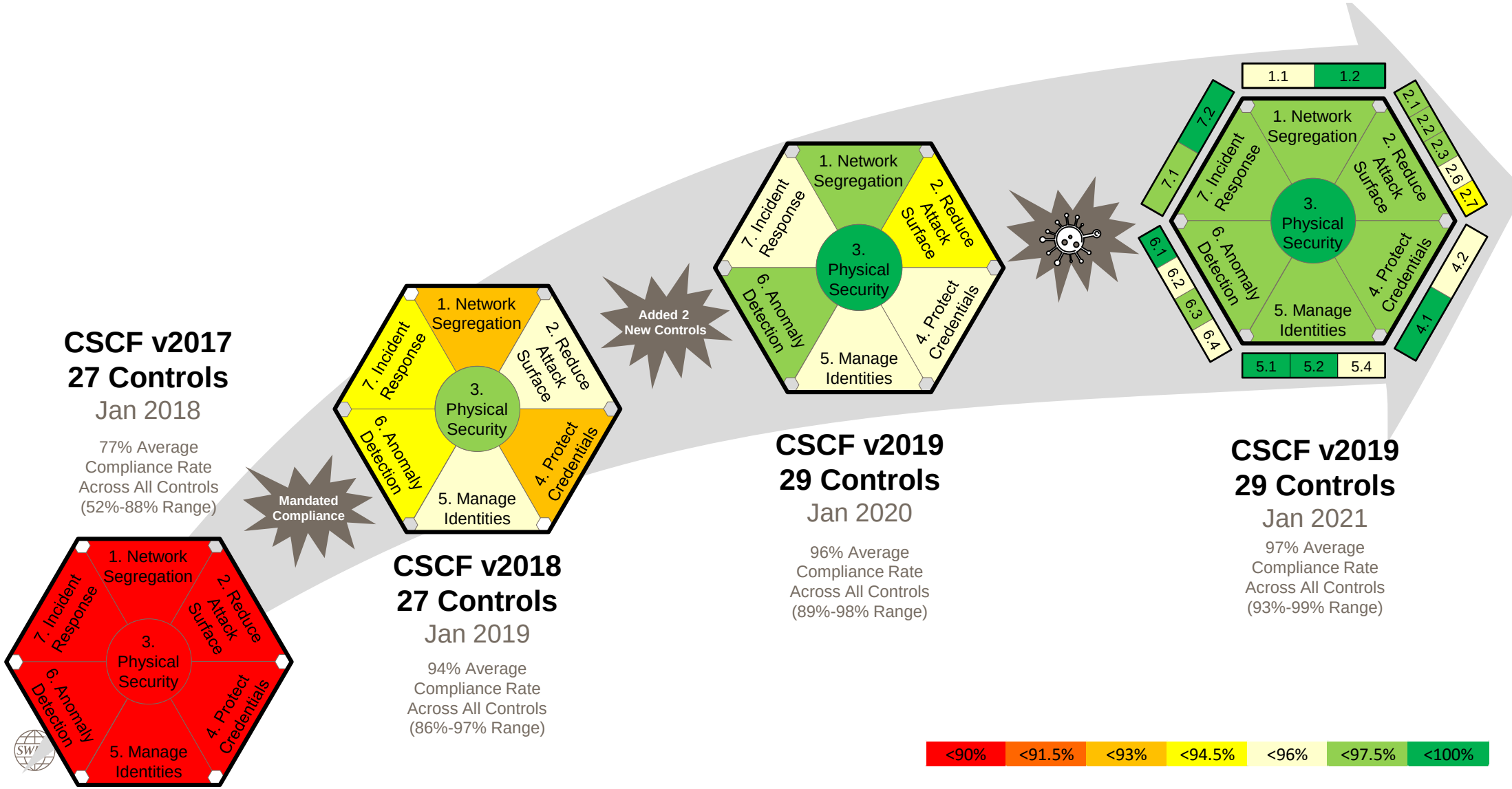






Customer Security Programme | Compliance Evolution

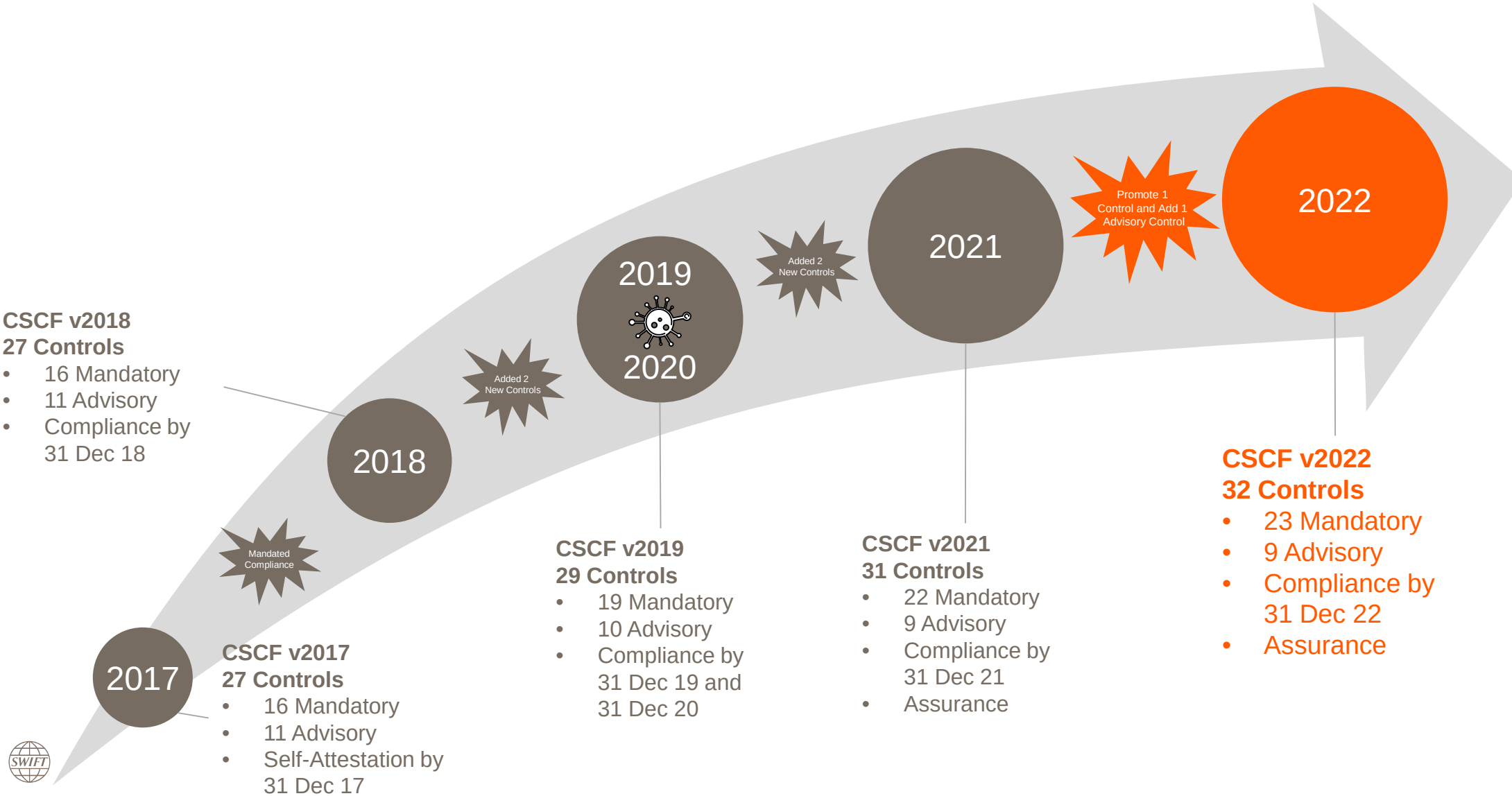
Customer Security Programme



Customer Security Programme
CSCF and IAF in 2021 and beyond

CSCF Controls | Evolution since 2017

Customer Security Programme



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

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

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	Architecture T…				
	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	•	•	•	•	•

1

2

CSCF v2022 | Most important changes

Customer Security Programme

1. **Promotion of Control 2.9A** (Transaction Business Controls) **to ‘mandatory’** after important scope and implementation guidelines clarifications

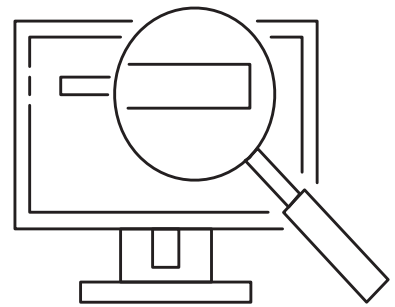
2. **New Advisory Control 1.5A** (Customer Environment Protection) to align requirements, of Architecture A4 with the other type ‘A’ Architectures

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**

Independent Assessment Framework in 2021 | Key changes

- 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**



www.swift.com