Customer Security Programme

CSP Update 2021

Sept 2020

Webinar Norms

- We welcome your kind participation. Thank YOU.
- We will start session at 15:05 SGT.
- Make sure you turn off your video.
- By default everyone will be muted.
- Note down your question. You can post it on Q&A Chat session.
- In interest of time, if your question can’t be addressed, we will get back to you via email.
- For any CSP queries post session, raise support case.
- This meeting will be recorded.

SWIFT

Customer Security Programme
CSP Update 2021

Sept, 2020

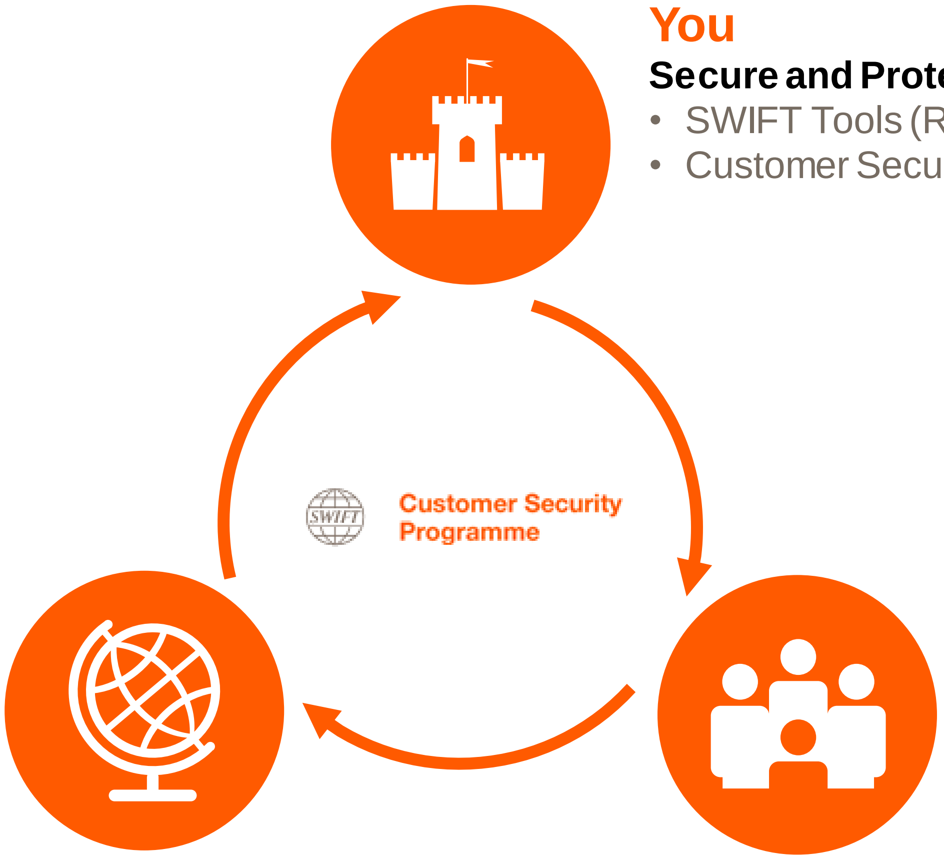
Agenda

- CSP - Evolution
- 2020 EOY KYC-SA Attestation
- CSCF v2021
- Independent Assessment Framework (IAF)
- Summary
- FAQ
- Resources

CSP - Evolution

CSP | Programme Reminder – Where does the CSCF stand?

Launched in 2016, CSP is designed to help SWIFT users implement practices that are essential to help protect against, detect and share information about financial services cybercrime.



You

Secure and Protect

- SWIFT Tools (R7.4; Security Guidance)
- Customer Security Controls Framework

Your Counterparts

Prevent and Detect

- RMA, DVR and ‘In Flight’ Sender Payment Controls Service
- KYC-SA application (request/review)
- Independent Assessment Framework

Your Community

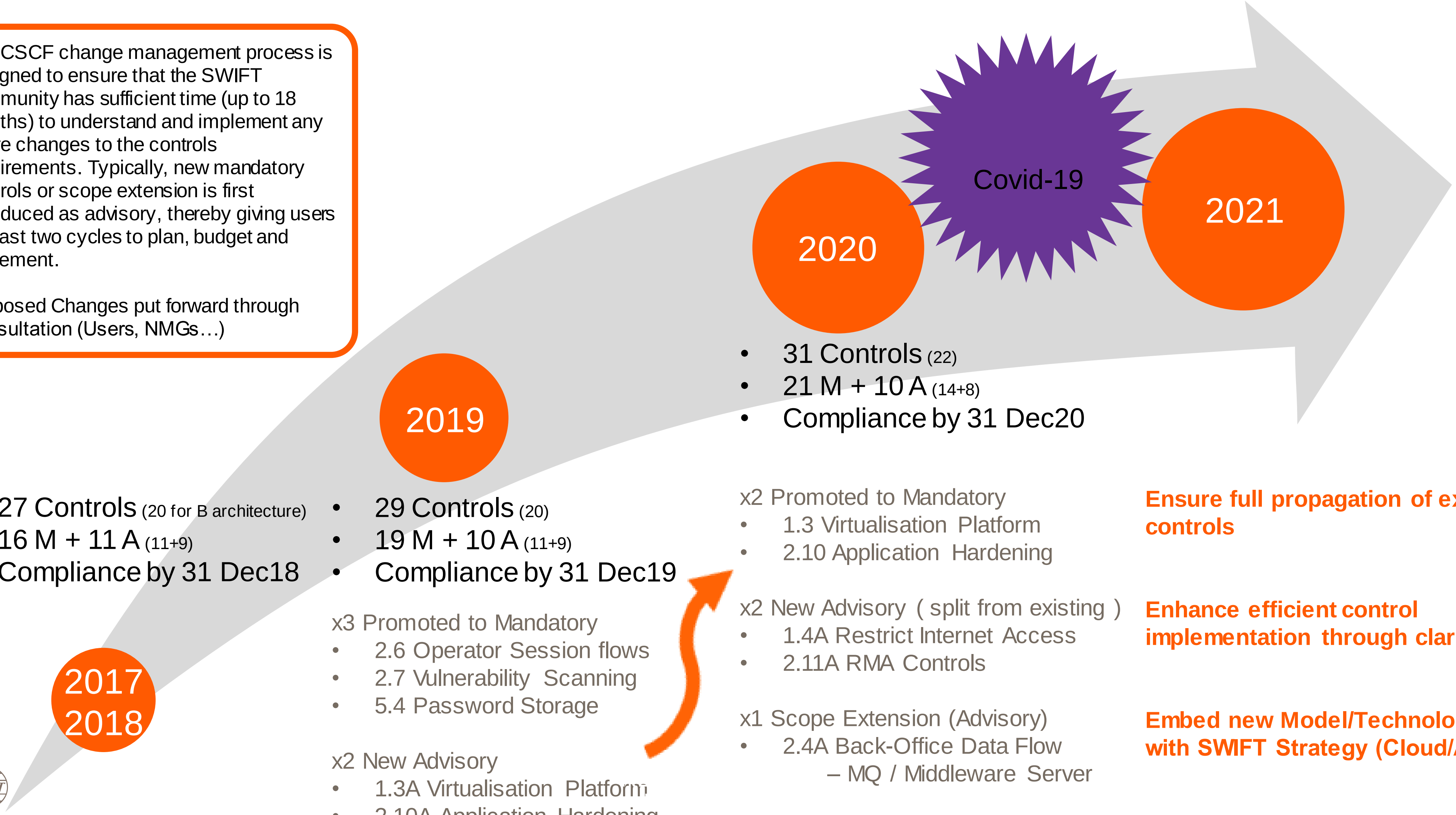
Share and Prepare

- Intelligence Sharing
- SWIFT ISAC Portal

CSCF v2021 | Pragmatically Raising the Bar – **Strategic Approach for v2021**

The CSCF change management process is designed to ensure that the SWIFT community has sufficient time (up to 18 months) to understand and implement any future changes to the controls requirements. Typically, new mandatory controls or scope extension is first introduced as advisory, thereby giving users at least two cycles to plan, budget and implement.

Proposed Changes put forward through Consultation (Users, NMGs…)



2017–2018

- 27 Controls (20 for B architecture)
- 16 M + 11 A (11+9)
- Compliance by 31 Dec18

2019

- 29 Controls (20)
- 19 M + 10 A (11+9)
- Compliance by 31 Dec19

x3 Promoted to Mandatory

- 2.6 Operator Session flows
- 2.7 Vulnerability Scanning
- 5.4 Password Storage

x2 New Advisory

- 1.3A Virtualisation Platform
- 2.10A Application Hardening

2020

- 31 Controls (22)
- 21 M + 10 A (14+8)
- Compliance by 31 Dec20

x2 Promoted to Mandatory

- 1.3 Virtualisation Platform
- 2.10 Application Hardening

x2 New Advisory (split from existing)

- 1.4A Restrict Internet Access
- 2.11A RMA Controls

x1 Scope Extension (Advisory)

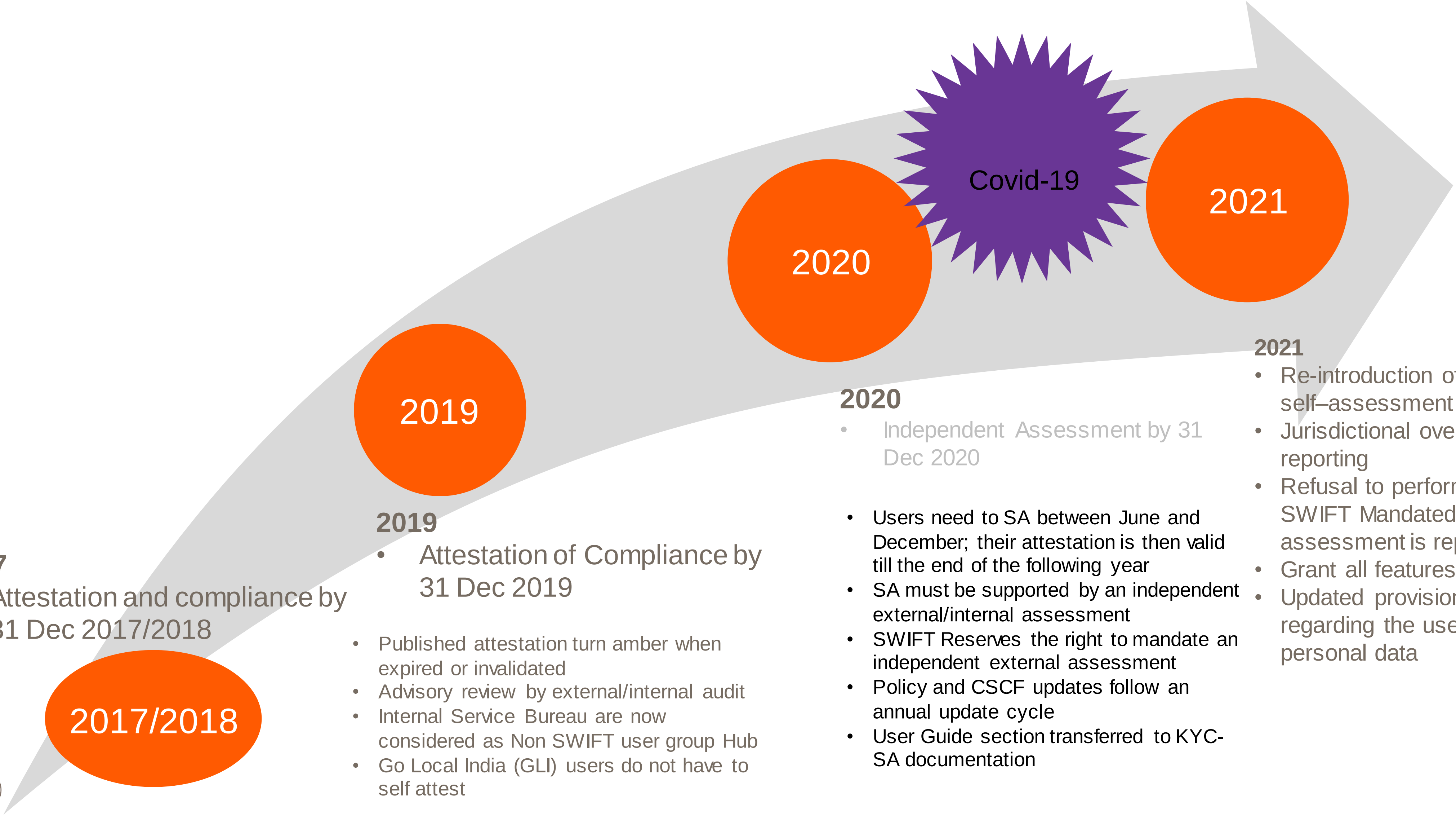
- 2.4A Back-Office Data Flow – MQ / Middleware Server

Ensure full propagation of existing controls

Enhance efficient control implementation through clarification

Embed new Model/Technology in line with SWIFT Strategy (Cloud/API's)

CSP | Policy Evolution



2017

- Attestation and compliance by 31 Dec 2017/2018

2019

- Attestation of Compliance by 31 Dec 2019

- Published attestation turn amber when expired or invalidated
- Advisory review by external/internal audit
- Internal Service Bureau are now considered as Non SWIFT user group Hub
- Go Local India (GLI) users do not have to self attest

2020

- Independent Assessment by 31 Dec 2020

- Users need to SA between June and December; their attestation is then valid till the end of the following year
- SA must be supported by an independent external/internal assessment
- SWIFT Reserves the right to mandate an independent external assessment
- Policy and CSCF updates follow an annual update cycle
- User Guide section transferred to KYC-SA documentation

2021

- Re-introduction of the self–assessment option
- Jurisdictional overseers reporting
- Refusal to perform a SWIFT Mandated assessment is reportable
- Grant all features
- Updated provisions regarding the use of personal data

2020 EOY KYC-SA Attestation

CSP | CSCF v2019 remains valid for 2020 attestation cycle

EOY Attestation

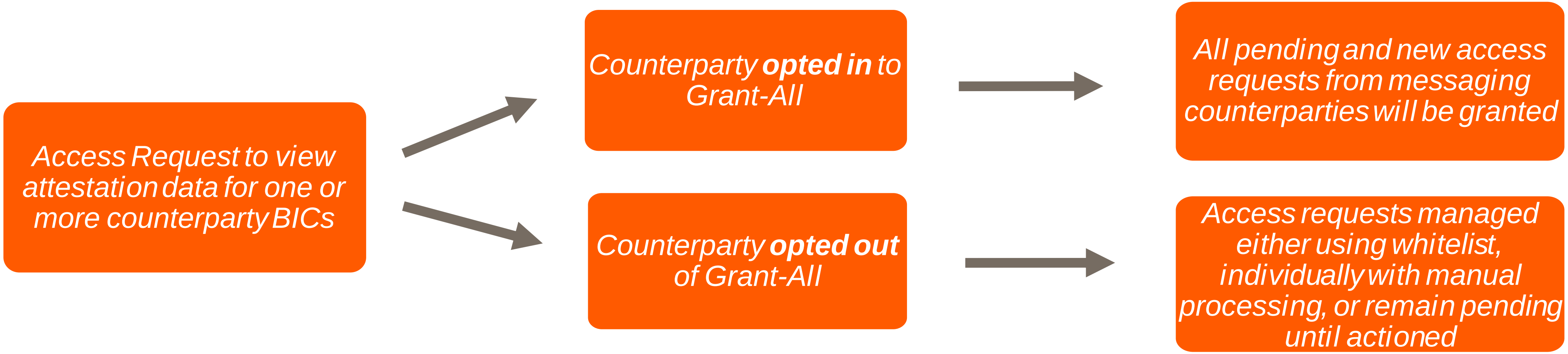
- Users are requested to **attest against the CSCF v2019** during the second half of 2020
  - KYC-SA baseline 2019.3 to be used in KYC-SA, available since 1st July 2020
  - IAF is **not** mandated in 2020
  - Congratulations to Users who have already completed their 2020 KYC attestation in KYC-SA
  - Users who have not submitted their attestation, are encouraged to do so as early as possible, but no later than 31st Dec 2020
- SWIFT Mandated assessments invitations will be sent out in September 2020 and the assessments will be required to be completed by December 2021 against v2021
- For more information, refer the CSP Timelines Update FAQ, via KB Tip **5024006**

CSP | Grant All Features and Functions

‘Grant All’ objective: **To improve operational efficiency of sharing attestation data by allowing access to your attestation data for all pending and new access requests from messaging counterparties**

During an initial notice period of 2 months, ability for customer to opt-out of the ‘grant all’ capability. After the notice period of 2 months, remaining customers will be opted in by default.

- For customers opted in to ‘Grant all’, all incoming Access Requests from messaging counterparties will be ‘granted’
- All customers are opted in after the initial notice period, unless they choose to opt out
- If you are opted in after the initial notice period, you may opt out at any time
- Extend overview of active Counterparties to Granters & Security Officers
- Updated grid view of counterparties and request status



Access Request to view attestation data for one or more counterparty BICs

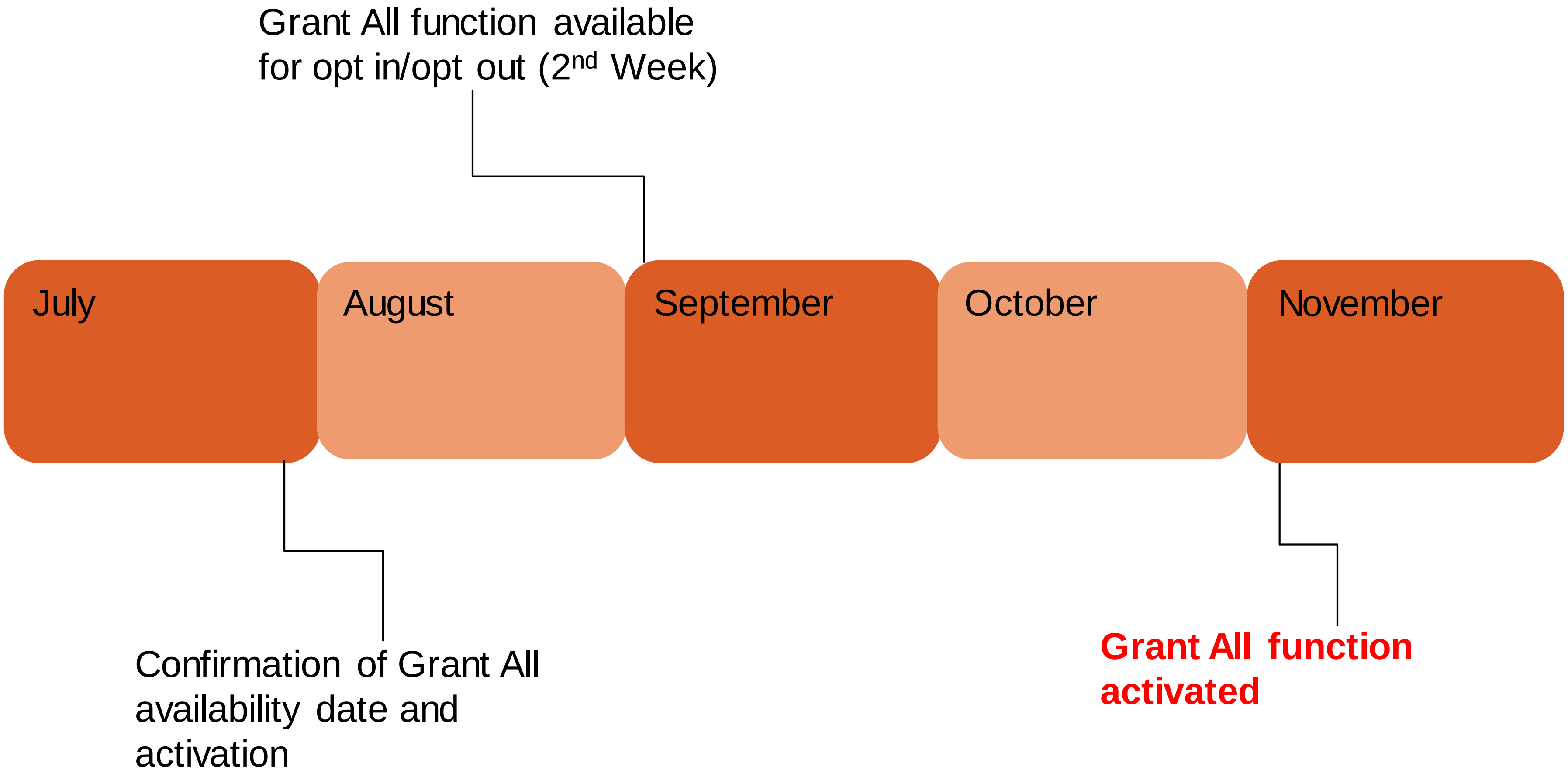
*Counterparty **opted in** to Grant-All*

All pending and new access requests from messaging counterparties will be granted

*Counterparty **opted out** of Grant-All*

Access requests managed either using whitelist, individually with manual processing, or remain pending until actioned

CSP | Grant All Implementation Timeline



Grant All function available for opt in/opt out (2nd Week)

July

August

September

October

November

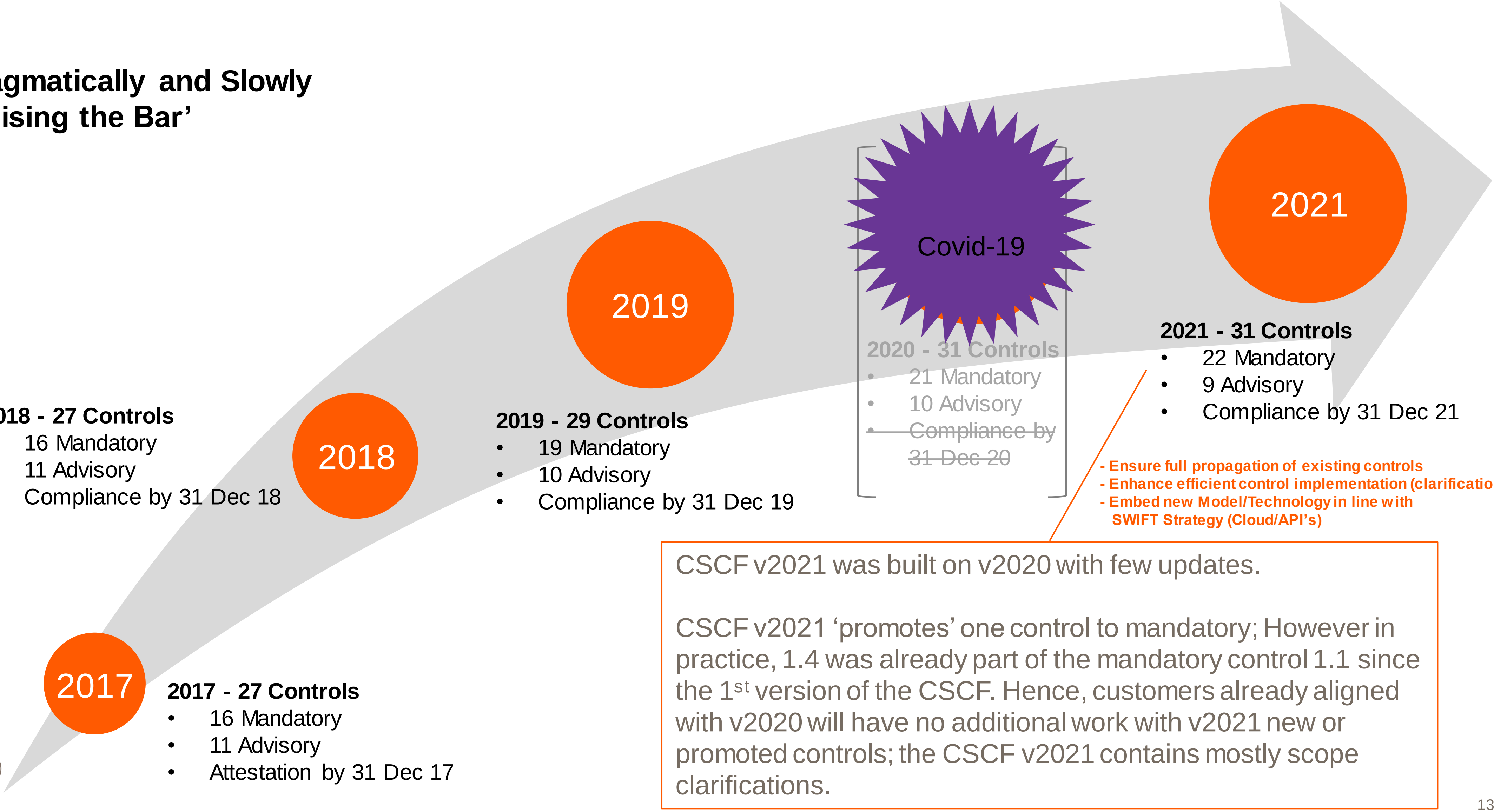
Confirmation of Grant All availability date and activation

Grant All function activated

CSCF v2021

CSCF Controls Evolution

Pragmatically and Slowly 'Raising the Bar'



2017 - 27 Controls
- 16 Mandatory
- 11 Advisory
- Attestation by 31 Dec 17

2018 - 27 Controls
- 16 Mandatory
- 11 Advisory
- Compliance by 31 Dec 18

2019 - 29 Controls
- 19 Mandatory
- 10 Advisory
- Compliance by 31 Dec 19

2020 - 31 Controls
- 21 Mandatory
- 10 Advisory
- ~~Compliance by 31 Dec 20~~

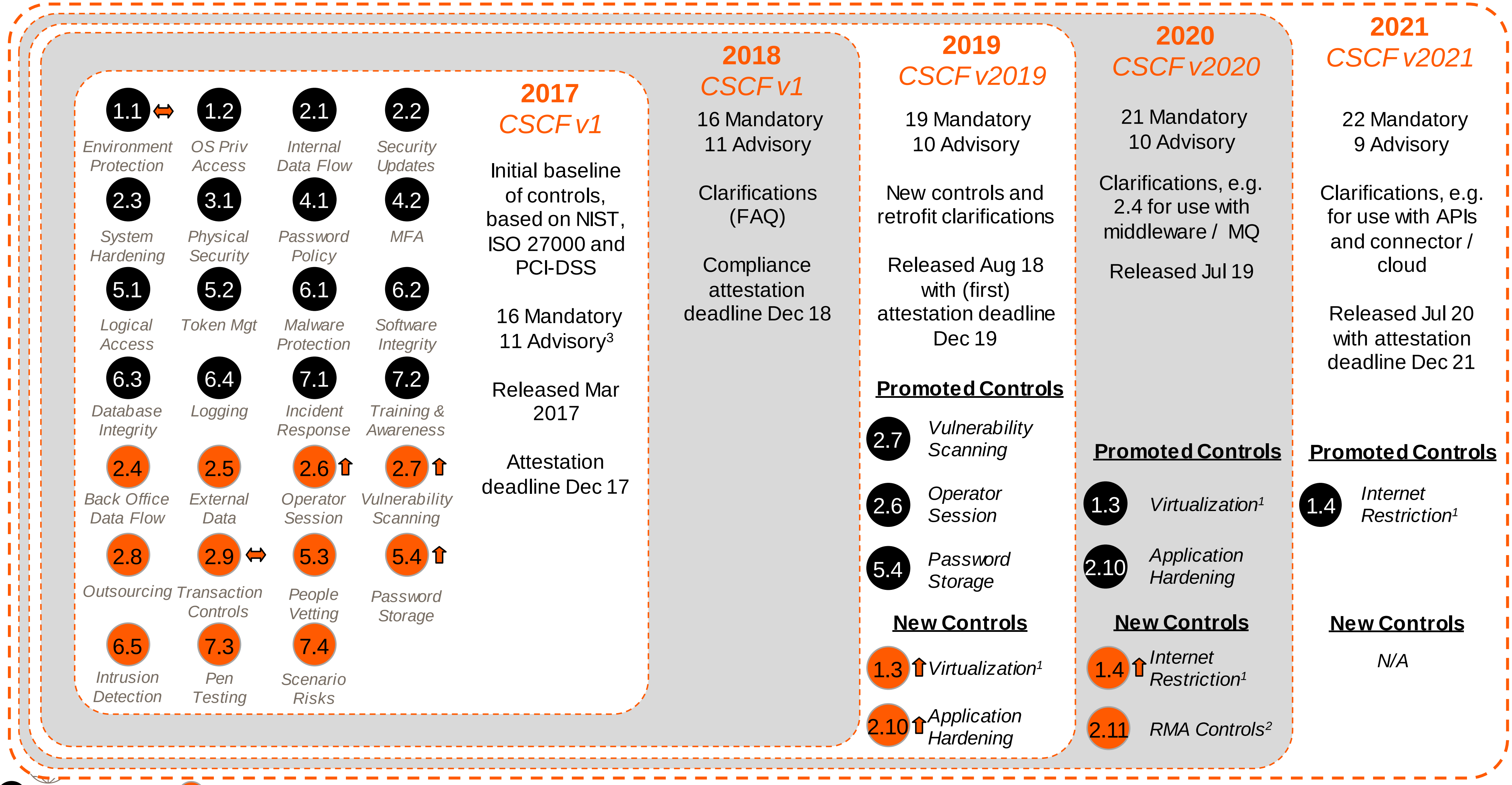
2021 - 31 Controls
- 22 Mandatory
- 9 Advisory
- Compliance by 31 Dec 21

- Ensure full propagation of existing controls
- Enhance efficient control implementation (clarifications
- Embed new Model/Technology in line with SWIFT Strategy (Cloud/API's)

CSCF v2021 was built on v2020 with few updates.

CSCF v2021 'promotes' one control to mandatory; However in practice, 1.4 was already part of the mandatory control 1.1 since the 1st version of the CSCF. Hence, customers already aligned with v2020 will have no additional work with v2021 new or promoted controls; the CSCF v2021 contains mostly scope clarifications.

Evolution of CSCF Controls – Pragmatically and Slowly 'Raising the Bar'



2017
CSCF v1

- 1.1 ⇔ Environment Protection
- 1.2 OS Priv Access
- 2.1 Internal Data Flow
- 2.2 Security Updates
- 2.3 System Hardening
- 3.1 Physical Security
- 4.1 Password Policy
- 4.2 MFA
- 5.1 Logical Access
- 5.2 Token Mgt
- 6.1 Malware Protection
- 6.2 Software Integrity
- 6.3 Database Integrity
- 6.4 Logging
- 7.1 Incident Response
- 7.2 Training & Awareness
- 2.4 Back Office Data Flow
- 2.5 External Data
- 2.6 ⇧ Operator Session
- 2.7 ⇧ Vulnerability Scanning
- 2.8 Outsourcing
- 2.9 ⇔ Transaction Controls
- 5.3 People Vetting
- 5.4 ⇧ Password Storage
- 6.5 Intrusion Detection
- 7.3 Pen Testing
- 7.4 Scenario Risks

Initial baseline of controls, based on NIST, ISO 27000 and PCI-DSS

16 Mandatory
11 Advisory[3]

Released Mar 2017

Attestation deadline Dec 17

2018
CSCF v1

16 Mandatory
11 Advisory

Clarifications (FAQ)

Compliance attestation deadline Dec 18

2019
CSCF v2019

19 Mandatory
10 Advisory

New controls and retrofit clarifications

Released Aug 18 with (first) attestation deadline Dec 19

Promoted Controls

- 2.7 Vulnerability Scanning
- 2.6 Operator Session
- 5.4 Password Storage

New Controls

- 1.3 ⇧ Virtualization[1]
- 2.10 ⇧ Application Hardening

2020
CSCF v2020

21 Mandatory
10 Advisory

Clarifications, e.g. 2.4 for use with middleware / MQ

Released Jul 19

Promoted Controls

- 1.3 Virtualization[1]
- 2.10 Application Hardening

New Controls

- 1.4 ⇧ Internet Restriction[1]
- 2.11 RMA Controls[2]

2021
CSCF v2021

22 Mandatory
9 Advisory

Clarifications, e.g. for use with APIs and connector / cloud

Released Jul 20 with attestation deadline Dec 21

Promoted Controls

- 1.4 Internet Restriction[1]

New Controls

N/A

● Mandatory Control ● Advisory Control ⇧ Control is subsequently promoted ⇔ Control is subsequently split

[1] 1.3 & 1.4 were split from 1.1

[2] 2.11 was split from 2.9

CSCF v2021 | Consultation Process and Summary of resulting Changes

Consultation Process

1 Who

~150 External Stakeholders

- Customers
- NMG's and country representatives
- Overseers through NBB

2 What

Scope Consideration

- Promotion of Advisory Controls to Mandatory?
- New Advisory Controls?
- Alternative implementations?
- Clarifications to cope with new technologies?

3 How

Via Webinars and Feedback Forms

- Regional webinars to introduce proposed changes
- Feedback Forms ~30 received - NMGs (13), Customers (12), Representatives (3)

Summary of CSCF v2021 Changes

New Controls - N/A

Ensure full propagation of existing controls

Fully Transfer Internet Access from Mandatory 1.1 to 1.4

1.4 – Restrict Internet Access.

- Centralise guidance related to internet access
- Remove *existing scope* from initial Control 1.1

Protect Operator PCs, initial targets before lateral move
Reduction of 1.1 and transfer to 1.4 was already defined in CSCF v2020

Clarifications on scope definition

General

- Ease identification of elements in scope
- Highlight risk-based approach for compliance
- Connector definition review (SWIFT <> Customer ones)

General Operator PC's

- Highlight PC's connected to local or remote infrastructure need to be protected

APIs – No change today but pave for the future

- Back office still out of scope with SWIFT footprint
- New Architecture Type - A4 for customer's own connectors (middleware or API end point)

Third Party – Extended to cloud provider

- Highlight where reasonable comfort has to be sought from the used Cloud Provider – User still accountable
- Support to Digital Connectivity

Split usage of SWIFT footprint (A1/A2/AA3) from customer's connectors (A4)

SWIFT footprint: products delivered by SWIFT and vendors (SAA/AMH/SAG/SIL/DL/MicroGateway)

CSCF v2021 – Rationale for the new Architecture A4

Today's Architectures and Limitations

A1/A2

Interfaces

SWIFT Footprint

- SWIFT or vendors' compatible Products to link with SWIFTNet
- SAG/AGI/SAA/AMH in Secure Zone
- All controls

A3

Connectors

SWIFT Footprint

- SWIFT or Compatible Vendors Software to connect Interfaces at Service Provider or Lite2
- (SIL)DL/AC/MicroGateway in Secure Zone
- All but 1 control

Other Footprint progressively in

- File transfer solutions, local middleware servers to connect with Service Provider
- Less controls (Advisory)

A3…

Limitations

Mix of SWIFT and non-SWIFT

- Difficult to extend the scope
- Mix of Mandatory <> Advisory
- API model will extend usage of Non-SWIFT Footprint

Split A3 between SWIFT & Non-SWIFT Footprint

Connectors: local software to facilitate communication with an interface, or to a service provider
Differentiate
SWIFT connectors - provided by SWIFT or vendors - SWIFT Footprint e.g. Autoclient, SIL
Customer connectors - off the shelf (file transfer solutions, Middleware/MQ servers…) or home made product (implementing API's) - Non-SWIFT footprint

A3 Architecture - relies on SWIFT connectors
(New) **A4 Architecture** - relies on Customer connectors

Controls with Clarified In-Scope

A3 – No Change

- Same controls as today - SWIFT connector in-scope

A4 – Introduced as Advisory to pave the way

- Controls with customer connector in-scope
  - Basic Cyber Hygiene
  - Connectivity for local App2app
  - Centralised business controls
- Scope can be progressively wider

Benefits

- Better split to ease proper architecture identification by users
- Differentiate pace of changes
- Pave the way for future models (no SWIFT-Footprint with API's)
- Could allow to identify and cover other intermediate actors (third party)

CSCF v2021 – Architecture A3 versus New Architecture A4

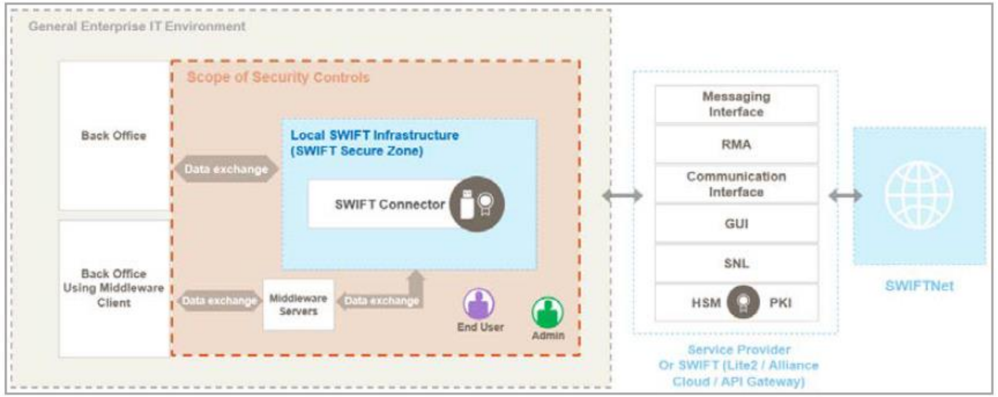

General Enterprise IT Environment
Scope of Security Controls
Back Office
Data exchange
Local SWIFT Infrastructure (SWIFT Secure Zone)
SWIFT Connector
Back Office Using Middleware Client
Data exchange
Middleware Servers
Data exchange
End User
Admin
Messaging Interface
RMA
Communication Interface
GUI
SNL
HSM
PKI
Service Provider Or SWIFT (Lite2 / Alliance Cloud / API Gateway)
SWIFTNet

Figure 5: Architecture A3 – SWIFT Connector

SWIFT Connector: products delivered by SWIFT and potentially vendors (DirectLink, AutoClient, SIL, MicroGateway)

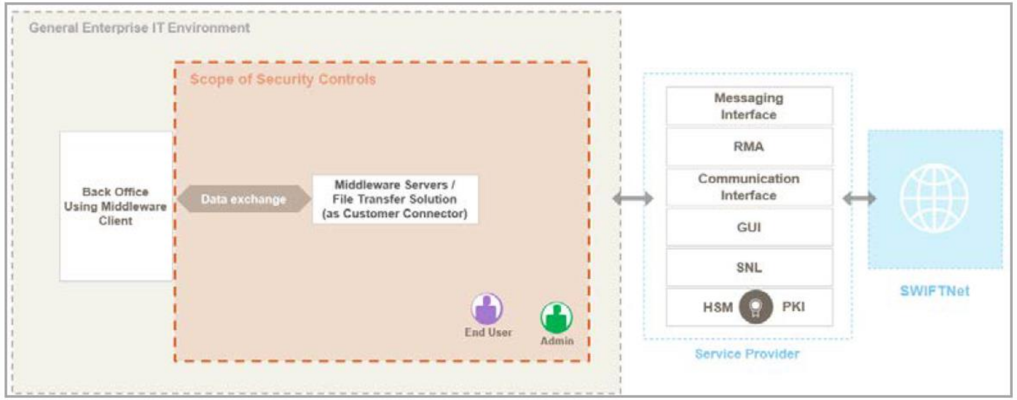

General Enterprise IT Environment
Scope of Security Controls
Back Office Using Middleware Client
Data exchange
Middleware Servers / File Transfer Solution (as Customer Connector)
End User
Admin
Messaging Interface
RMA
Communication Interface
GUI
SNL
HSM
PKI
Service Provider
SWIFTNet

Figure 6a: Architecture A4 – Middleware/File Transfer as Connector

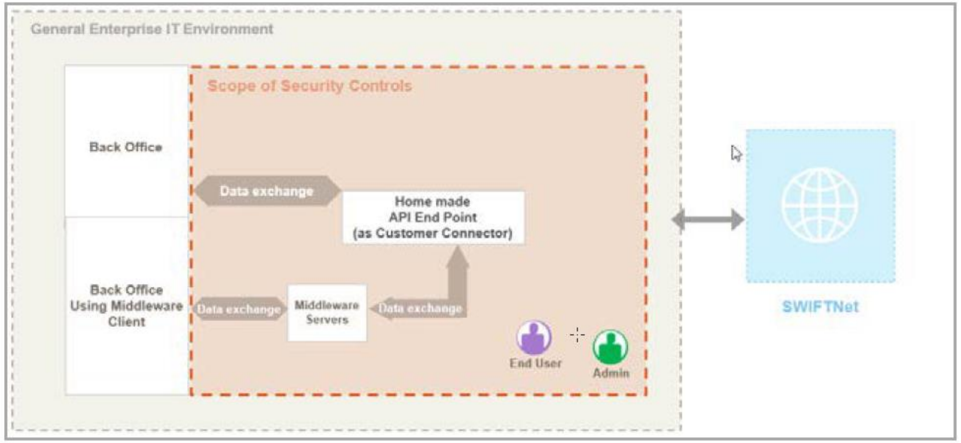
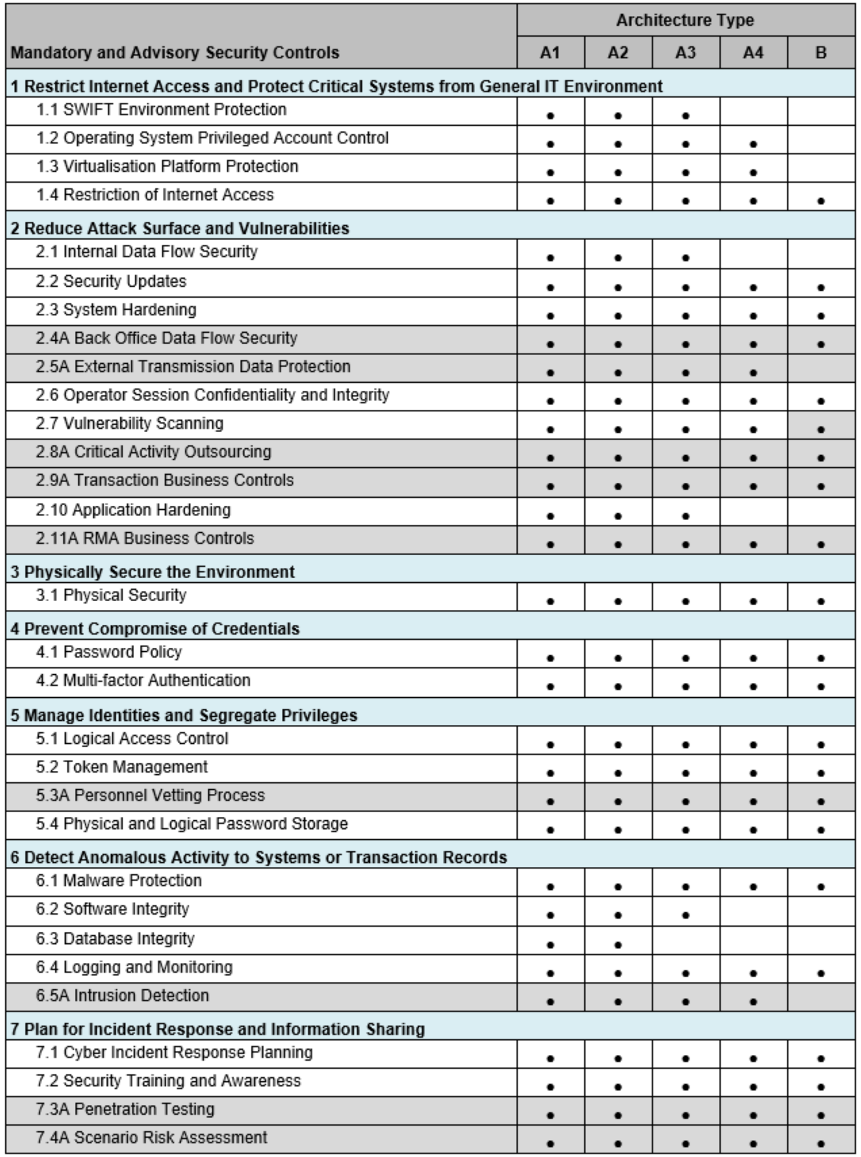

General Enterprise IT Environment
Scope of Security Controls
Back Office
Data exchange
Home made API End Point (as Customer Connector)
Back Office Using Middleware Client
Data exchange
Middleware Servers
Data exchange
End User
Admin
SWIFTNet

Figure 6b: Architecture A4 – Customer (home-made API) Connector

CSCF v2021 – Summary and Controls Applicability

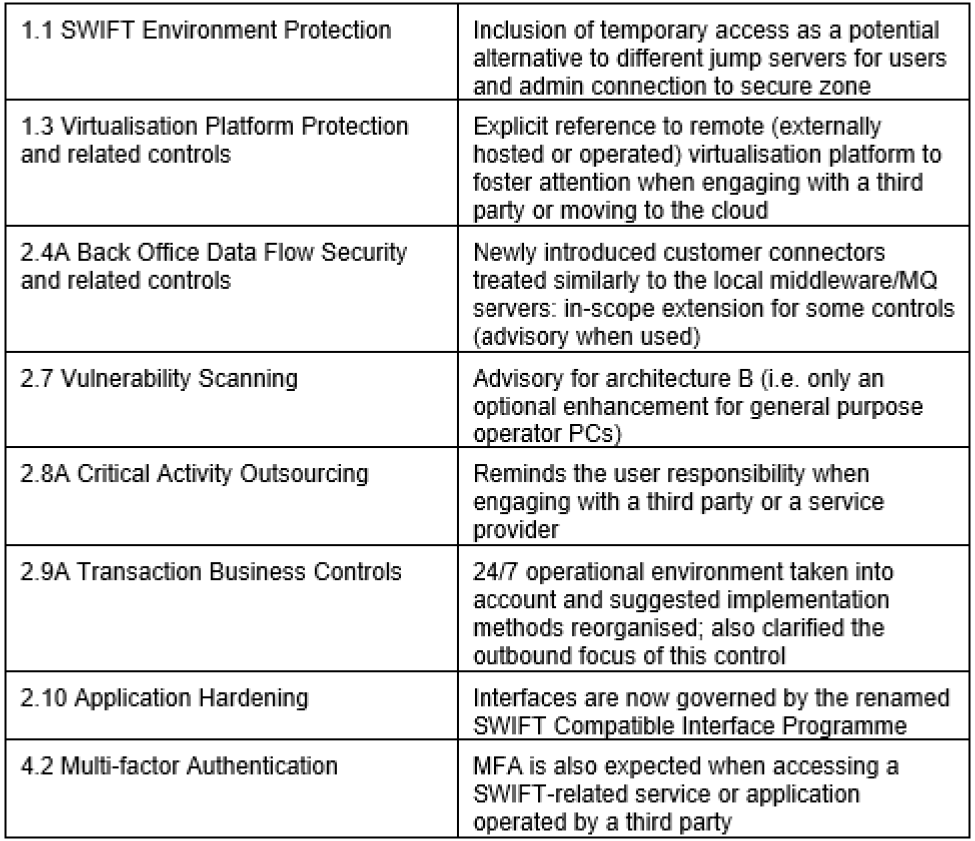


Mandatory and Advisory Security Controls	Architecture Type				
	A1	A2	A3	A4	B
1 Restrict Internet Access and Protect Critical Systems from General IT Environment					
1.1 SWIFT Environment Protection	●	●	●		
1.2 Operating System Privileged Account Control	●	●	●	●	
1.3 Virtualisation Platform Protection	●	●	●	●	
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	●	●	●	●	●

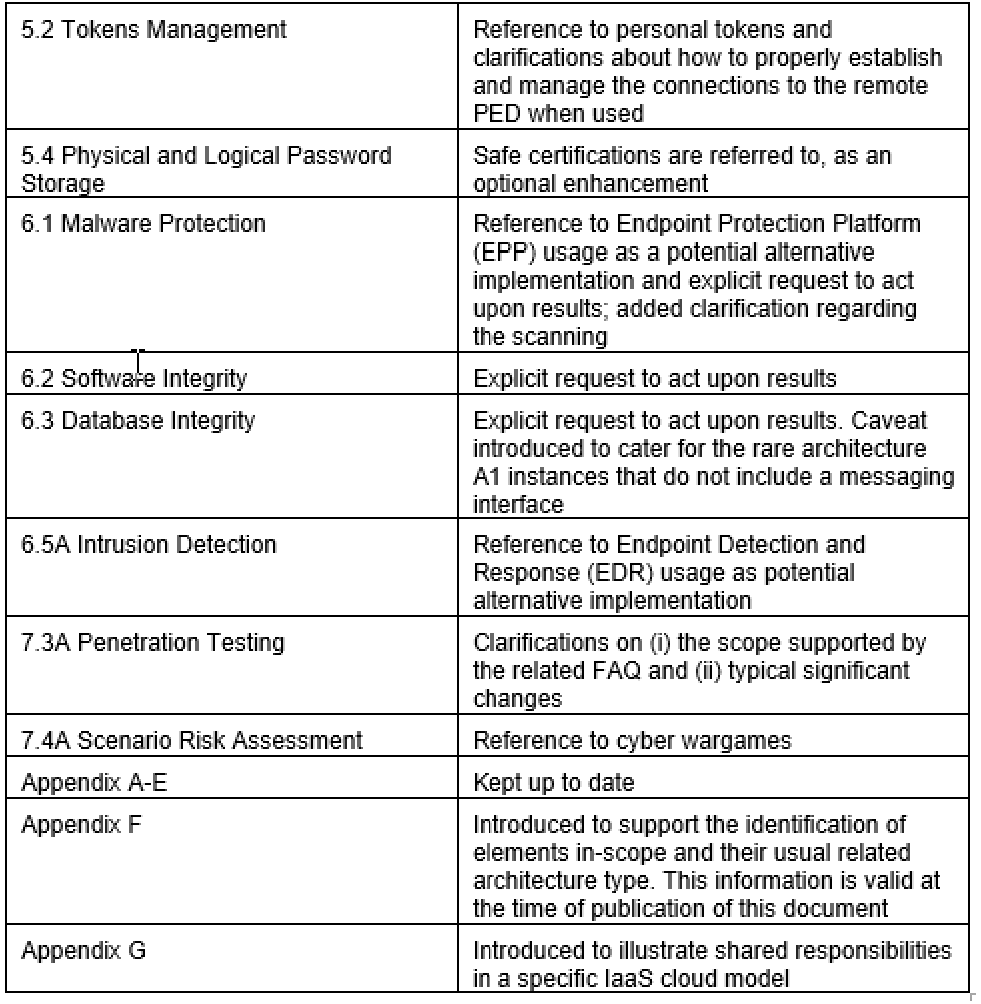
Arch	A1	A2	A3	A4	B
Man.	22	22	21	17	14
Adv.	9	9	9	9	8
Tot.	**31**	**31**	**30**	**26**	**22**

Consider also Annex F of CSCF v2021 for controls applicability

CSCF v2021 – Clarifications for Efficiency and Alignment to Reality



1.1 SWIFT Environment Protection	Inclusion of temporary access as a potential alternative to different jump servers for users and admin connection to secure zone
1.3 Virtualisation Platform Protection and related controls	Explicit reference to remote (externally hosted or operated) virtualisation platform to foster attention when engaging with a third party or moving to the cloud
2.4A Back Office Data Flow Security and related controls	Newly introduced customer connectors treated similarly to the local middleware/MQ servers: in-scope extension for some controls (advisory when used)
2.7 Vulnerability Scanning	Advisory for architecture B (i.e. only an optional enhancement for general purpose operator PCs)
2.8A Critical Activity Outsourcing	Reminds the user responsibility when engaging with a third party or a service provider
2.9A Transaction Business Controls	24/7 operational environment taken into account and suggested implementation methods reorganised; also clarified the outbound focus of this control
2.10 Application Hardening	Interfaces are now governed by the renamed SWIFT Compatible Interface Programme
4.2 Multi-factor Authentication	MFA is also expected when accessing a SWIFT-related service or application operated by a third party



5.2 Tokens Management	Reference to personal tokens and clarifications about how to properly establish and manage the connections to the remote PED when used
5.4 Physical and Logical Password Storage	Safe certifications are referred to, as an optional enhancement
6.1 Malware Protection	Reference to Endpoint Protection Platform (EPP) usage as a potential alternative implementation and explicit request to act upon results; added clarification regarding the scanning
6.2 Software Integrity	Explicit request to act upon results
6.3 Database Integrity	Explicit request to act upon results. Caveat introduced to cater for the rare architecture A1 instances that do not include a messaging interface
6.5A Intrusion Detection	Reference to Endpoint Detection and Response (EDR) usage as potential alternative implementation
7.3A Penetration Testing	Clarifications on (i) the scope supported by the related FAQ and (ii) typical significant changes
7.4A Scenario Risk Assessment	Reference to cyber wargames
Appendix A-E	Kept up to date
Appendix F	Introduced to support the identification of elements in-scope and their usual related architecture type. This information is valid at the time of publication of this document
Appendix G	Introduced to illustrate shared responsibilities in a specific IaaS cloud model

Independent Assessment Framework (IAF)

CSP | Flavours of the assessments

Assessment Type	Selection Criteria	Assessor	Timeline			
			2019	2020	2021	2022 and beyond
❶ Self-Assessment	Still possible but will not be compliant after start of IAF	First Line of defense	🟩	🟩	🟩🟧	🟧 Non Compliant-reportable as of Jan2022
❸ Community-Standard Assessment	Mandated for all customers with the start of IAF	Internal or external			🟩	🟩
❸ SWIFT-Mandated Assessment	Mandated - Sampled Customers Driven by QA Analysis	External only	▨	▨	▨	▨

Start of IAF

CSP | Audit vs Assessment

The objective is the same: providing assurance on the compliance with the stated CSCF **Control Objective**.

- The two approaches (Audit / Assessment) are possible:
  - Assessments are more **flexible** and there is a **wider range of assessment providers**, including those who may not necessarily meet the requirements of an audit organisation.
  - **Audit** is subject to **internationally recognised standards**. An audit is typically **longer** and more **expensive** than an assessment.

- SWIFT is **indifferent on** the way assurance is provided (assessment or audit) provided the firm (and the individual assessors) possess the necessary skills as set out in the independent Assurance Framework.

CSP | Risk-Based approach when assessing security compliance

Assessors must employ a **risk-based approach** when assessing the security compliance of the users; i.e. assessors must not use the SWIFT proposed Implementation Guidelines as a strict audit check list.

Hence, **the implementation of a CSP control can be:**

- As per the documented SWIFT proposed Implementation Guidelines
- An alternative Implementation that:
  - Addresses the risk drivers
  - Covers the relevant in-scope components
  - Meets the stated control objective, i.e. the security goal to be achieved

IMPORTANT: Both methods are **valid and equivalent** from a CSP compliance perspective

CSP | Independent Assurance Framework flow and timeline

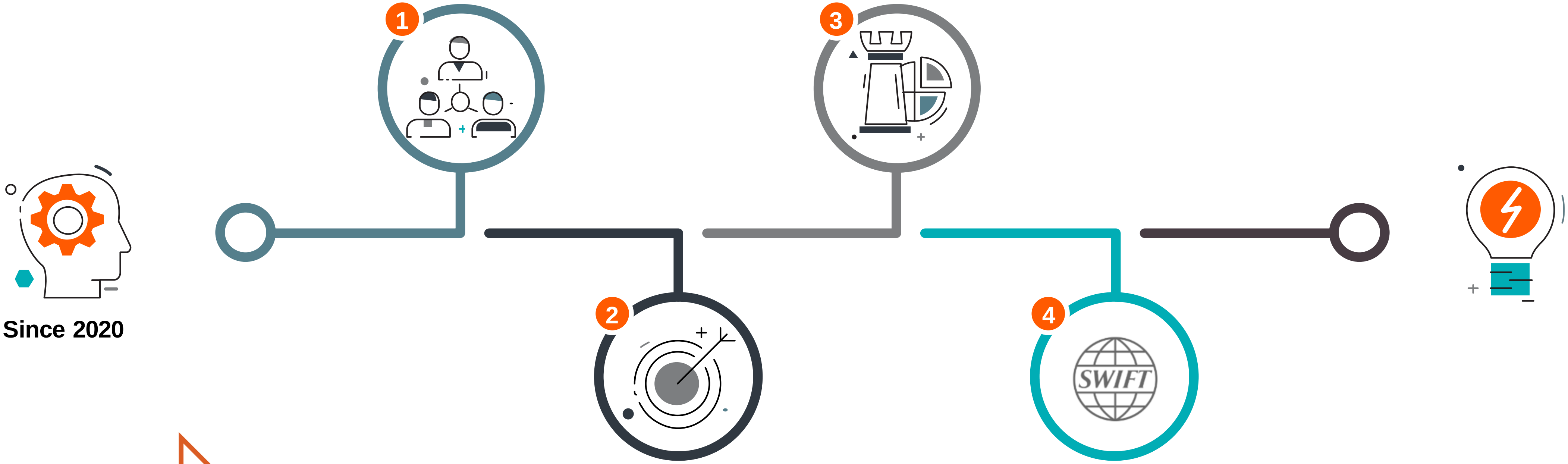
Independent assessor selection

- Customer to select an internal OR/AND external assessor
- For an external assessor, customers can consult the Directory of CSP Assessment Providers

Results reflected in the KYC-SA application

Upon availability of the controls version in the application (as from July 1st)

- Customer to align their self attestation results against the review results
- Customer to add the name and contact details of assessor and start and end date of the assessment report



Since 2020

Against the current CSCF version of the controls

Assessor conducts review

- Customer and assessor to apply the framework and Word and excel templates as described in the KC.
- Customer can consult FAQ KB TIP 5022902 or contact SWIFT Support
- Use future version of the CSCF for clarifications as appropriate

Escalation

- Failure to undertake a Community-Standard assessment before the end of the calendar year 2021 will result in a non compatible attestation and reporting to the local supervisors and visible to counterparties via the KYC-SA application
- An assessment will have a validity period of maximum two years under conditions

CSP | Independent Assurance Framework – details (1/2)

	Community-Standard Assessments All customers from 2021 Internal or external assessment
Assessor must have Skills	• **Independency**: as defined by 'Institute of Internal Auditors' (IIA) • **Recent (12 months) and relevant experience**, e.g. PCI DSS, ISO 27001 • **Qualifications**, e.g. QSA, CISSP, CISA, CISM, or similar
Assessor Selection	• **Internal** independent assessor: **second or third line of defence** or its functional equivalent • **External** assessors: (non-prescriptive) **directory of CSP assessment providers** • **Service providers** such as service bureaus or L2BA provider are **eligible** under some conditions • SWIFT **does not endorse or validate** any particular assessor
Available Resources	• CSP SWIFTSmart **modules** (translations available) • Swift.com KC: PDF Framework document, Optional Excel-based *Assessment Templates* and *Word Completion letter* • CSP **curriculum** (Annex A of the IAF)

CSP | Independent Assurance Framework – details (2/2)

	Community-Standard Assessments All customers from 2021 Internal or external assessment
Testing Methods	• **Risk-Based approach** (i.e. compliance vs control objective) • A **mix of assessment methods** as appropriate, e.g. interview, replay, documentation • Possible **leverage** of **existing relevant assurance**
Timing	• **Assessment** to start **any** time **during the year** • **Fill in** 2021 attestations **between** 1st July and 31st December 2021
Outputs	• **Recommended**: findings in the Excel-based *Assessment Templates* and Completion letter • **Expected**: summary of findings in assessor report to customer • **Recommended retention of 5 years (minimum 2 years)** of documentation
Escalation	• **Absence** of assessment results in **reporting to the supervisors** and visibility to counterparties
Costs	• **Customer** is **responsible** for **costs** associated with the assessment

Summary

CSP | COVID-19 : Expectation from Customers in 2020

Customer Security Programme

DO'S

- When attesting between July 2020 and December 2020, Users MUST use the CSCF v2019. SWIFT recommends to use the v2020 or the v2021 for clarifications only and at user's discretion; Consulting the published v2020 or v2021 must not result in any scope creep in 2020.
- Focus on the controls which are applicable this year for data attestation against **CSCF v2019.**
- Since attesting window in KYC-SA (baseline 2019.3) opens up on 1st July 2020, **ensure that you submit your attestation at the earliest.** Attestation submitted 1st July 2020 onwards, will have its validity till 31st Dec 2021, (Thus not limited to 12 months anymore).
- If you are a first time user, please ensure that you have access to KYC-SA application and you have identified and assigned designated users to perform data contribution to KYC-SA. Please refer the slides "How SWIFT can Help", for more information and further assistance.
- If you have not started working on your 2020 attestation yet, please initiate process, as we are heading towards Year End.
- Ensure that you are using the correct draft version any time in the process. This avoid re-work at your end.
- Once your attestation draft is finalized & submitted to the approver internally, please request the Approver to approve draft.
- If your Entity is managed centrally and intend to submit data attestation centrally, follow-up with your Parent BIC and remind them to submit data.
- If you are hosting SWIFT infrastructure for an attesting user, please help your hosted entity by proactively furnishing all required information needed to complete their attestation.
- Read the Tip **5024006** IAF FAQ COVID-19, if unsure about the impact on CSP timelines

CSP | Expectation from Customers

DON'TS

- Don't wait for last minute data submission in December, due to various reasons, such as:
  - Staff unavailability due to unforeseen sick leaves or planned personal leaves.
  - Year end resource crisis at customer end, due to long Christmas festival, in some regions.
  - Unforeseen emergencies/crisis at customer end will ideally takes precedence over data submission and attestation.

Through these Do's and Don'ts, SWIFT wants to re-iterate that it's a collaborative journey and without your genuine efforts, SWIFT may not be able to safeguard community from emerging Cyber Security threats at any given time. Your Co-operation is highly appreciated.

F
A
Q

CSP | FAQ

Compared to CSCFv2019, how many new mandatory & advisory controls introduced in CSCFv2021?

With the introduction of Architecture type A4 in CSCF v2021, is there a need to reassess one’s Architecture type, before data submission for July 2021 onwards?

With the introduction of Architecture type A4 in CSCF v2021, which existing Architecture type can have potential impact, for which reassessment required?

We are in middle of data attestation submission process for YR 2020 & SWIFT is now referring CSCF v 2021/IAF. What should be community focus and priority?

Is the (internal/external) independent assessment mandatory for 2021?

SWIFT has also Published CSCF v2020, document. Should one refer CSCF v2020 document along with CSCF v2021 document or just CSCF v2021, in preparation to next year attestation cycle?

I have been informed by SWIFT to perform “Mandated External assessment for YR 2021”, How should I proceed forward?

Form July 2021, Under the Assurance type, if one select “Self assessment”, will it be considered as non-compliant?

How SWIFT can help

CSP | Supporting the Community

Where can I go to find additional info?

swift.com*

* Login required

CSP Pages

Visit the CSP pages for programme news and updates. In particular:

- Filter the Latest news with “Customer Security Programme” and/or “Cyber Security” for relevant topics

Knowledge Centre

- Access all the CSP docs
- Access all the CSCF docs
- Access some additional supporting docs and modules

Knowledge Base

- Tip 5024006 IAF FAQ COVID-19
- **Tip** 5024038 CSP Timelines Update COVID-19
- Tip 5021823: CSP FAQ
- Tip 5022902: IAF FAQ
- Tip 5020786 Security Guidance

SWIFT ISAC Portal

Consult the Portal for information related to security threats

SWIFTSmart

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

Include a module related to the IAF

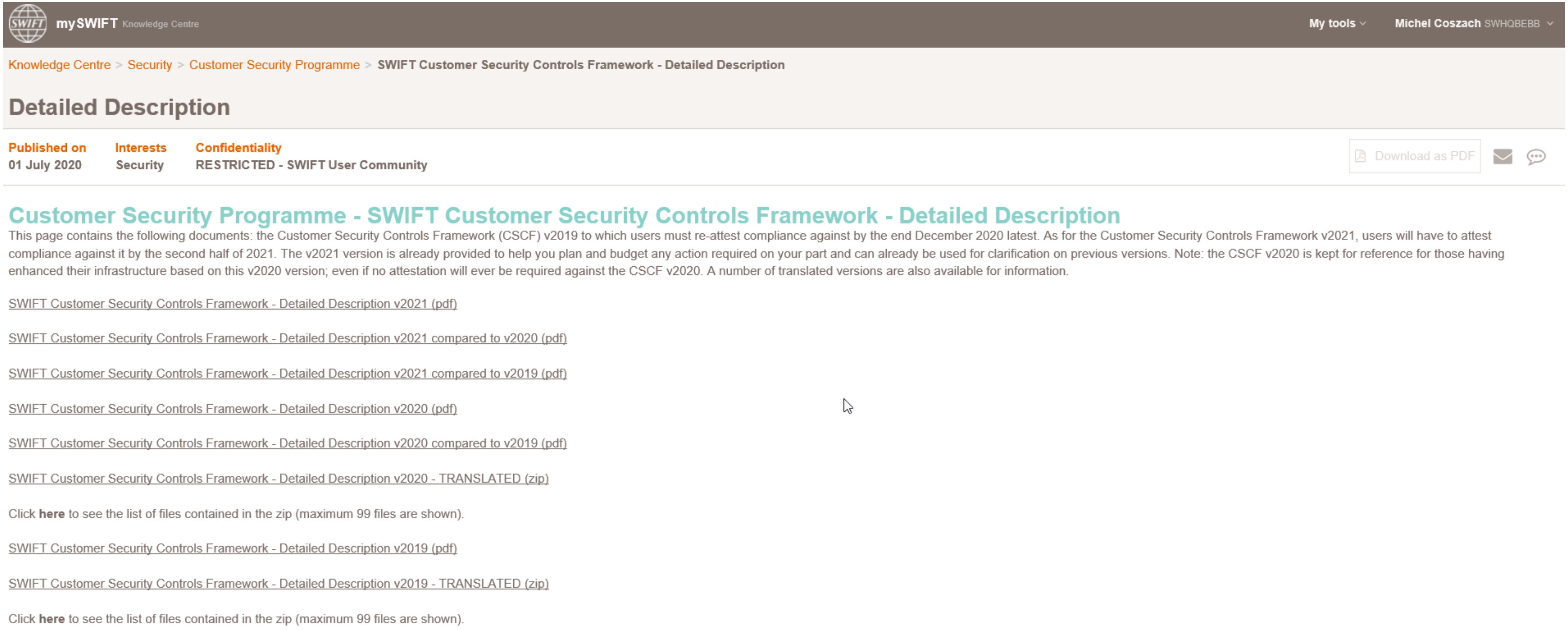
MySWIFT

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

CSP | Supporting the Community

Where can I go to find additional info?

Customer Security Programme



Knowledge Centre > Security > Customer Security Programme > SWIFT Customer Security Controls Framework - Detailed Description

Detailed Description

Published on	Interests	Confidentiality
01 July 2020	Security	RESTRICTED - SWIFT User Community

Customer Security Programme - SWIFT Customer Security Controls Framework - Detailed Description

This page contains the following documents: the Customer Security Controls Framework (CSCF) v2019 to which users must re-attest compliance against by the end December 2020 latest. As for the Customer Security Controls Framework v2021, users will have to attest compliance against it by the second half of 2021. The v2021 version is already provided to help you plan and budget any action required on your part and can already be used for clarification on previous versions. Note: the CSCF v2020 is kept for reference for those having enhanced their infrastructure based on this v2020 version; even if no attestation will ever be required against the CSCF v2020. A number of translated versions are also available for information.

SWIFT Customer Security Controls Framework - Detailed Description v2021 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2021 compared to v2020 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2021 compared to v2019 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2020 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2020 compared to v2019 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2020 - TRANSLATED (zip)

Click **here** to see the list of files contained in the zip (maximum 99 files are shown).

SWIFT Customer Security Controls Framework - Detailed Description v2019 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2019 - TRANSLATED (zip)

Click **here** to see the list of files contained in the zip (maximum 99 files are shown).

CSP | Supporting the Community

Need more help?

SWIFT

SWIFT Customer Support

SWIFT Customer Support teams are on hand 24/7 to answer specific queries if you don't find the information resources you are looking for.

Directory of CSP Assessment Providers

If you need support to perform the Independent assessment, consult the Directory of CSP assessment providers on SWIFT.com to help find a third-party project partner that may be suitable for your needs.

Directory of Cyber Security Service Providers

If you need practical, on-the-ground implementation support, you can consult the Directory of Cyber Security Service Providers on SWIFT.com to help find a third-party project partner that may be suitable for your needs.

SWIFT Services

To support best practices in infrastructure implementation and management SWIFT offer services such as the SWIFT infrastructure security review, Security boot camps, SWIFT Admin and Operation certifications and recurring support contracts such as Alliance Managed Operations, Local support and Premium custom support. Consult the Services page.

QUIZ

CSP | Quiz

1) Though we are in year 2020, KYC data-attestation this year is based on CSCF v2019 controls ?
True/False.

2) Independent Assessment, is mandated by SWIFT for year 2020 & as a customer I must work on this?
True/False

3) After the Nov Grant All activation, if the default "Opt In" is set in KYC-SA, access request (to attestation data) from messaging counterparties will be automatically processed/granted?True/False.

4) As per CSCF v2021 controls, there will be five architecture types going forward? True/False.

5) For performing community-standard assessment, any person can be approached to perform internal/external assessment? True/False

6) For performing community-standard assessment, customer is responsible for advance planning and budgeting? True/False

CSP | Quiz Answers

- Though we are in year 2020, KYC data-attestation this year is based on CSCF v2019 controls ?
  TRUE

- Independent Assessment, is mandated by SWIFT for year 2020 & as a customer I must work on this?
  FALSE

- After the Nov Grant All activation, if the default “Opt In” is set in KYC-SA, access request (to attestation data) from messaging counterparties will be automatically processed/granted?
  TRUE

- As per CSCF v2021 controls, there will be five architecture types going forward?
  TRUE

- For performing community-standard assessment, any person can be approached to perform internal/external assessment?
  FALSE

- For performing community-standard assessment, customer is responsible for advance planning and budgeting?
  TRUE

&

Feedback Poll is opened in parallel. Request you to please share your valuable Feedback, before you Leave.

CSP | Poll

1) Whether session was informative & met your expectation around CSP?
   a. Yes
   b. No

2) If the answer to above question is NO, please explain what was missed out and what you would like to hear more in upcoming session?

3) How would you like to rate this session?
   a. Very Satisfied
   b. Satisfied
   c. Unsatisfied

4) Any Feedback? (From CI perspective)

Your Feedback is Important

SWIFT

www.swift.com