Customer Security Programme

CSP Update v2021/2022

Webinar Norms

- We welcome your kind participation. Thank YOU.
- We will start session at XX:XX 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 a support case.
- This meeting recording & slide will be made available in SWIFT KB TIP5024202

Customer Security Programme
CSP Update 2021- Refresher

Q4 2021

Agenda

› Threat landscape evolution

› CSP – Compliance evolution

› MISP

› Customer Security Control Framework v2021

› Independent Assessment Framework (IAF)

› Demo - IAF and KYC-SA Attestation Portal

› Highlights of the Customer Security Control Framework v2022

› FAQ and Q&A

› How SWIFT can help

Threat Landscape Evolution

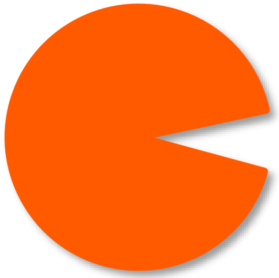
CSP | Measurable indicators showing CSP ‘effectiveness’

Overall Funds Attempted

dropped by factor of 3

2016 compared to 2020

Vast Majority of Funds are Recovered



All years

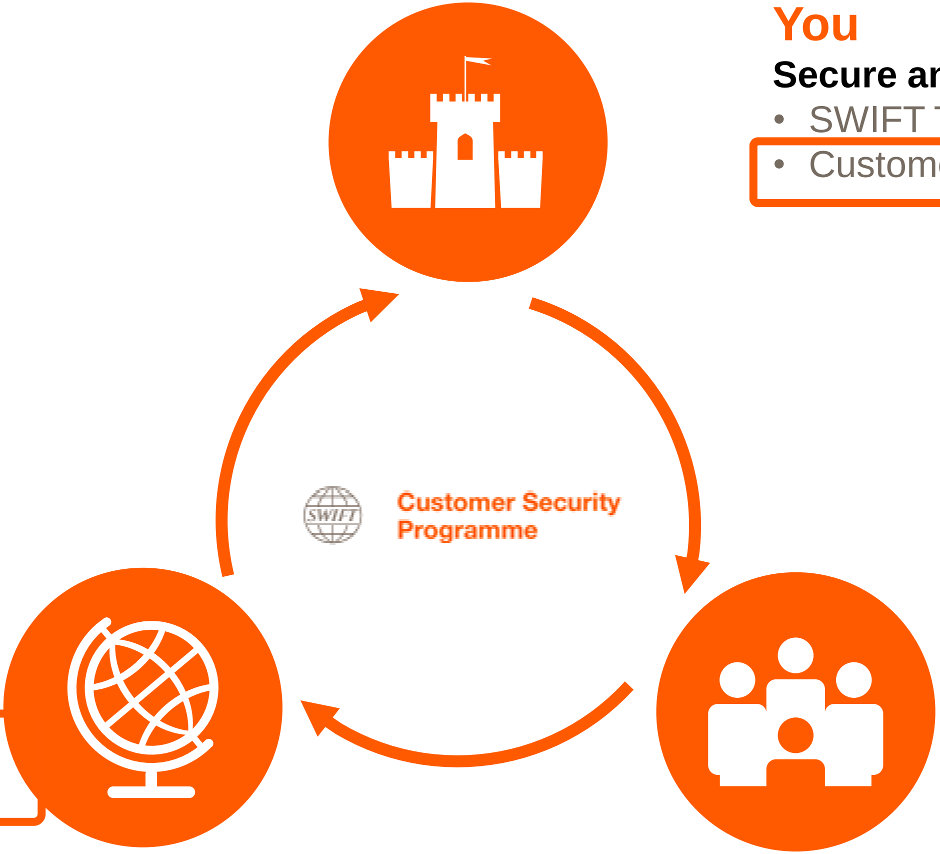
Trend is due to a Combination of Factors

1. Raised customer awareness
2. Implementation of the Controls
3. Hardened interfaces
4. Early detection of in-flight fraudulent messages
5. Strong collaboration across the chain

CSP – Compliance evolution

CSP | Programme Reminder – Where do the CSCF, IAF and MISP 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 (R7.5; Security Guidance)
- Customer Security Controls Framework

Your Counterparts

Prevent and Detect

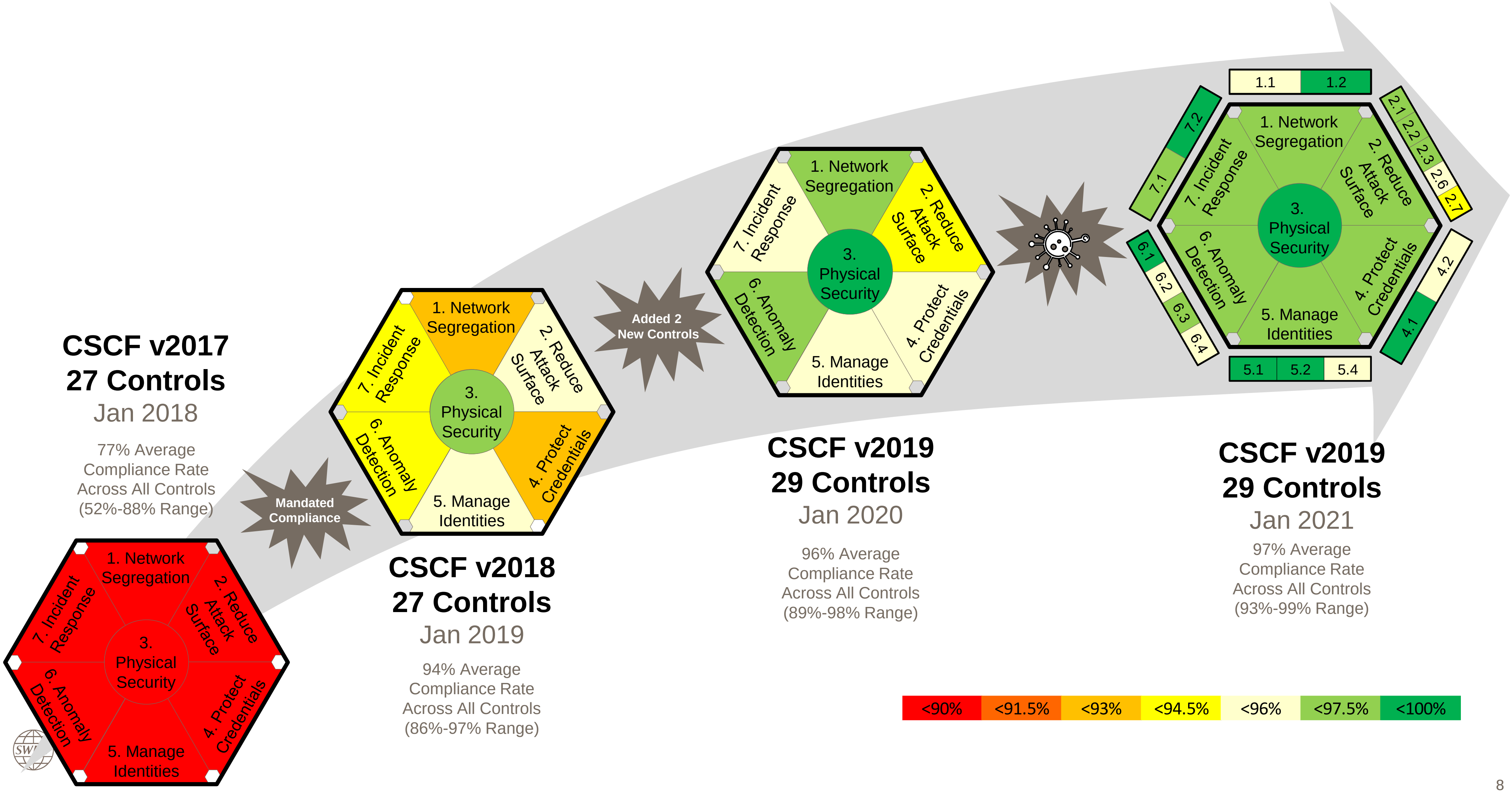
- RMA, DVR and 'In Flight' Sender Payment Controls Service
- KYC-SA application (request/review)
- Independent Assessment Framework

Your Community

Share and Prepare

- Intelligence Sharing
- SWIFT ISAC/MISP Portal

CSP | CSCF Controls Evolution



CSCF v2017
27 Controls
Jan 2018

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

CSCF v2018
27 Controls
Jan 2019

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

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)

🟥	🟧	🟧	🟨	⬜	🟩	🟩
<90%	<91.5%	<93%	<94.5%	<96%	<97.5%	<100%

MISP Migration

CSP | SWIFT ISAC/MISP Automated feed

MISP = Originally ‘malware information sharing platform’

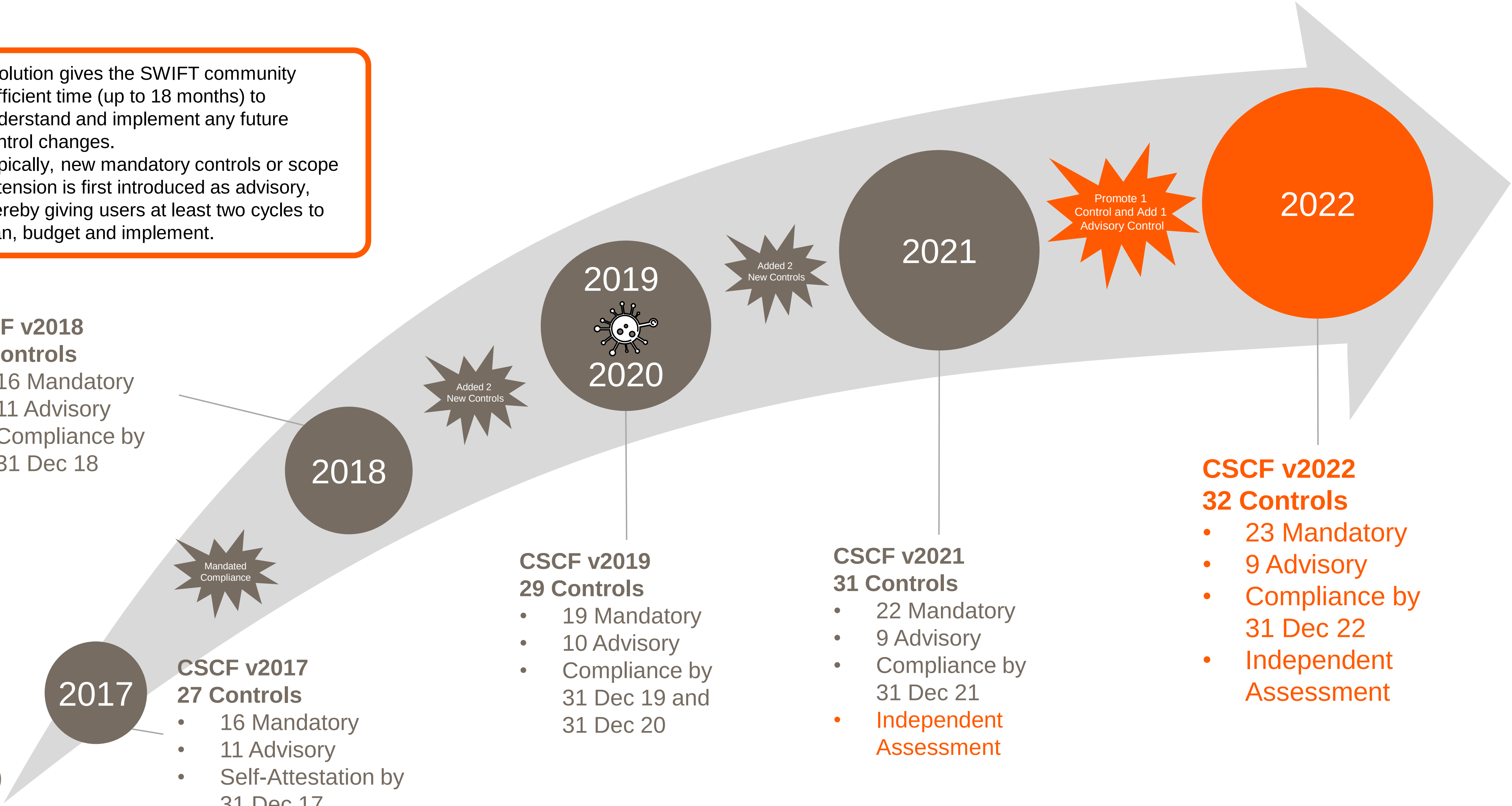
https://misp.swift.com/

- Free and open source
- Standard data format
- Threat intelligence platform capabilities
- REST API to export data in multiple formats
- Backed by European Commission
- Maintained by CIRCL (Luxemburg government CERT)
- Improves the way the IOCs are shared with the community
- Customers to pull the IOCs (Indicators of Compromise) from their own version of MISP
- SWIFT ISAC and MISP are complementary.

Customer Security Control Framework v2021

CSP | CSCF Controls Evolution

Evolution gives the SWIFT community sufficient time (up to 18 months) to understand and implement any future control changes.
Typically, new mandatory controls or scope extension is first introduced as advisory, thereby giving users at least two cycles to plan, budget and implement.



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
- Independent Assessment

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

CSCF v2021 | Key changes - overview

2 parts

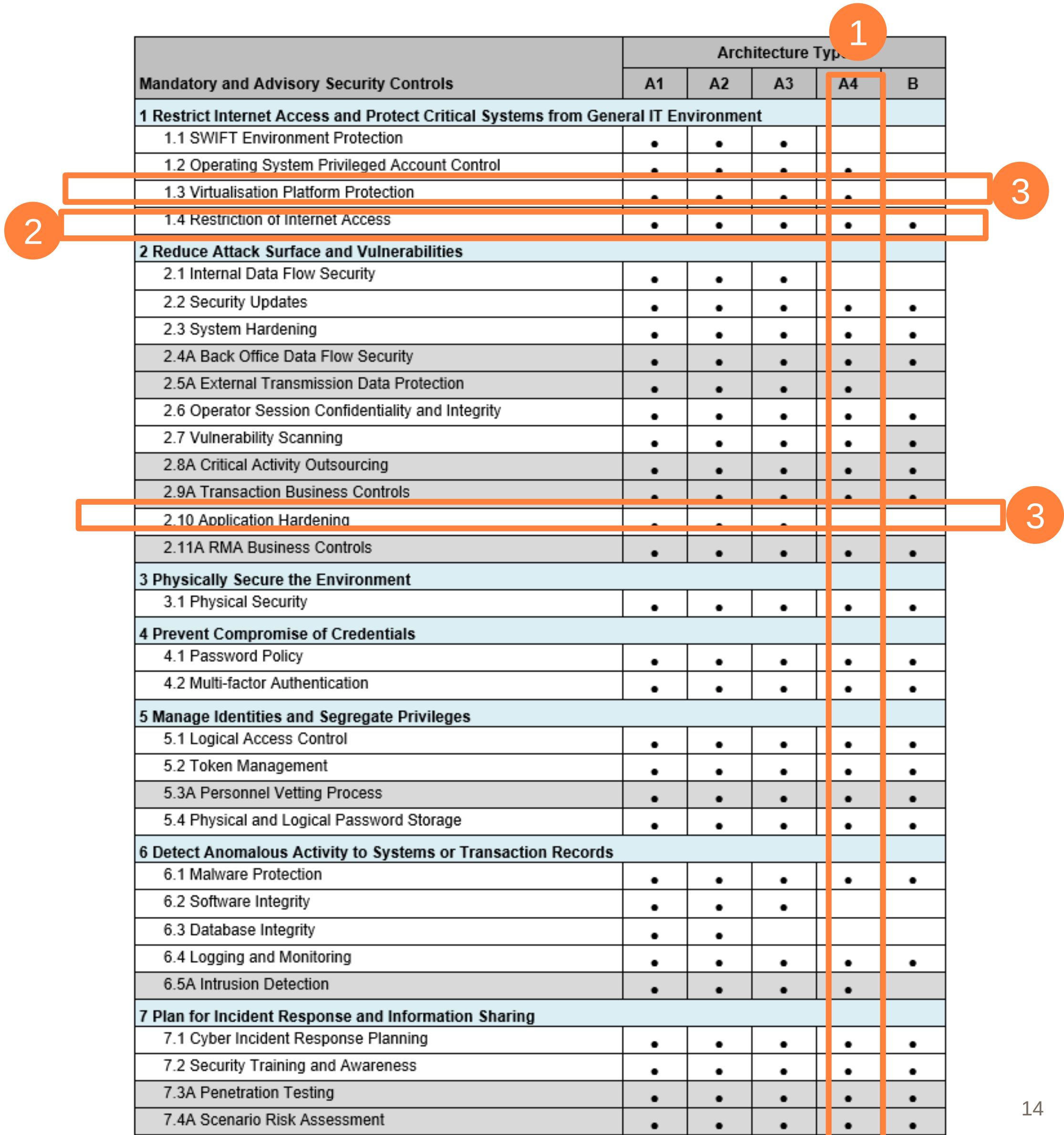
Raise the Security Bar – Scope change

Clarifications – Efficiency and alignment to reality

CSCF v2021 | Key changes - part 1

Raise the Security Bar – Scope change

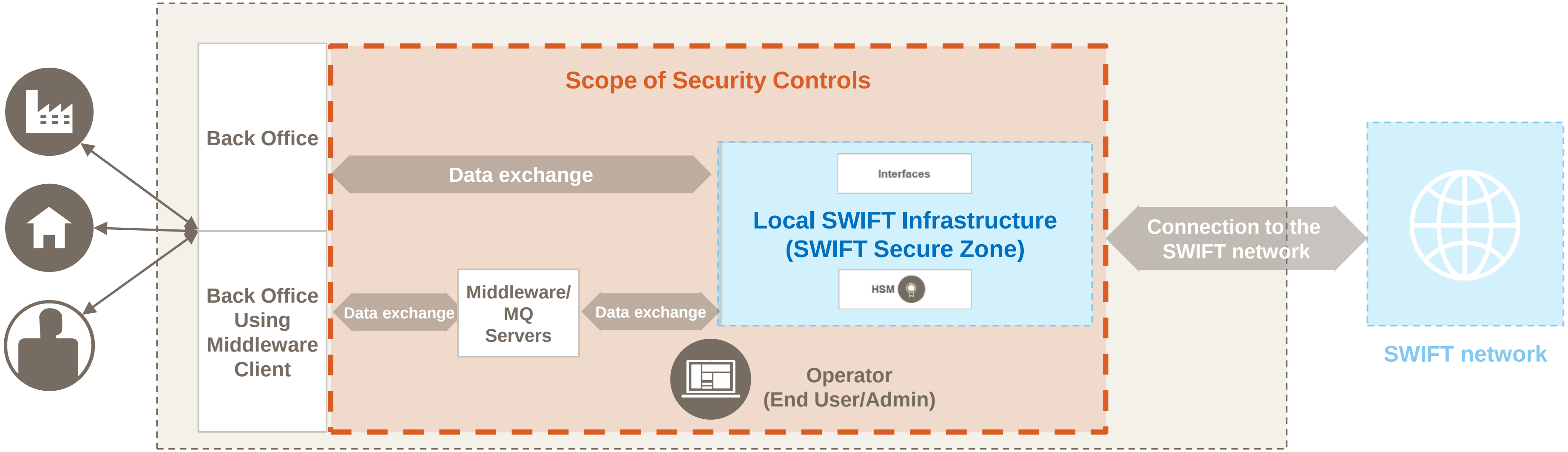
1. **Introduced Architecture type A4**
2. **Fully transfer ‘Internet Access’ provisions from control 1.1 to 1.4 (Restrict Internet Access)**
    - Centralize guidance related to internet access in 1.4
    - Remove *existing scope* from 1.1
3. **Compared to v2019**
    - Control 1.3 Virtualization platform turned mandatory
    - Control 2.10 Application Hardening platform turned mandatory



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	•	•	•	•	•

CSCF v2021 | CSP Scope in the CSCF v2020

User Environment (Architecture A1, A2, A3, with local footprint)

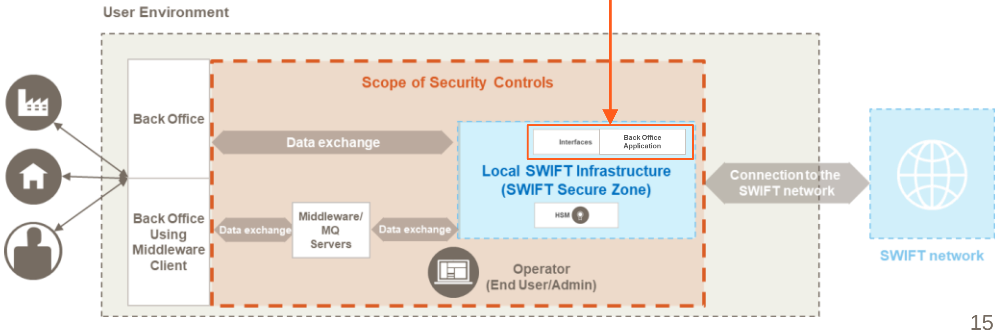


Back Office
Back Office Using Middleware Client
Scope of Security Controls
Data exchange
Interfaces
Local SWIFT Infrastructure (SWIFT Secure Zone)
HSM
Data exchange
Middleware/ MQ Servers
Data exchange
Operator (End User/Admin)
Connection to the SWIFT network
SWIFT network

Back Office definition:
“Systems responsible for business logic, transaction generation, and other activities occurring before transmission.”

➔ In general Out of Scope

Pay attention:
If a **Back Office** application is **cohosted with** an **Interface**, the **hosting system** (and its accesses) **is In Scope**.



User Environment
Back Office
Back Office Using Middleware Client
Scope of Security Controls
Data exchange
Interfaces
Back Office Application
Local SWIFT Infrastructure (SWIFT Secure Zone)
HSM
Data exchange
Middleware/ MQ Servers
Data exchange
Operator (End User/Admin)
Connection to the SWIFT network
SWIFT network

CSCF v2021 | Existing v2020 architecture types 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 footprint

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

CSCF v2021 | Scoping and benefits of introducing the new architecture type A4

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
  - Centralized business controls
- Scope can be progressively extended

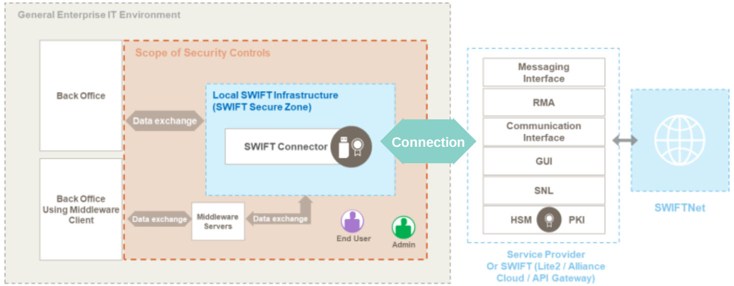
Benefits of the split A3 and A4 are:

- Facilitates the proper identification of the relevant architecture type by users
- Helps differentiate the pace of changes by SWIFT
- Paves the way for future models (no SWIFT-Footprint with API's)
- Could allow to identify and cover other intermediate actors (third party)

CSCF v2021 | Introduction of architecture A4 with CSCF v2021

Architecture A3 - SWIFT connector (provided by SWIFT, or holding a SWIFT-compatible label)

A3


General Enterprise IT Environment
Scope of Security Controls
Back Office
Back Office Using Middleware Client
Data exchange
Local SWIFT Infrastructure (SWIFT Secure Zone)
SWIFT Connector
Connection
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

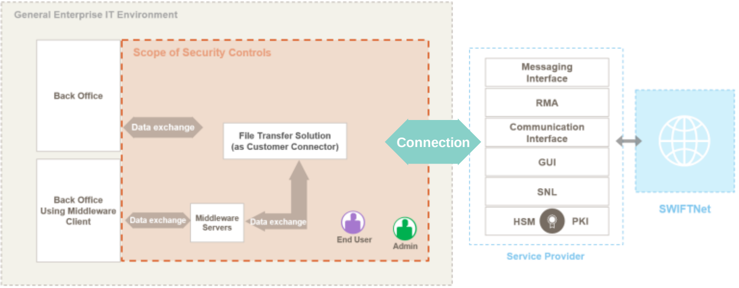
To connect to Lite2 (Alliance Cloud)

- (SIL)DirectLink
- AutoClient
- SWIFT Microgateway

in a Secure Zone

Architecture A4 - "Non-SWIFT" components Customer Connector - (developed in-house, or by a 3rd party vendor and not holding a SWIFT-compatible label)

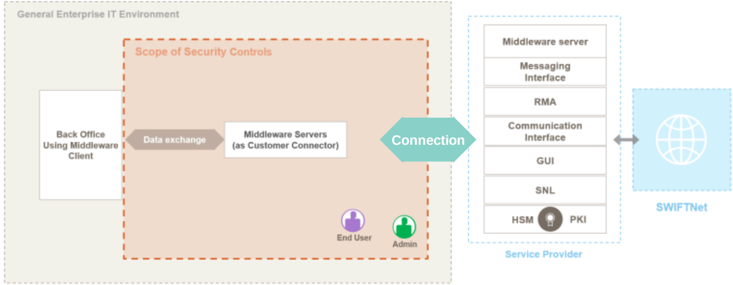
A4



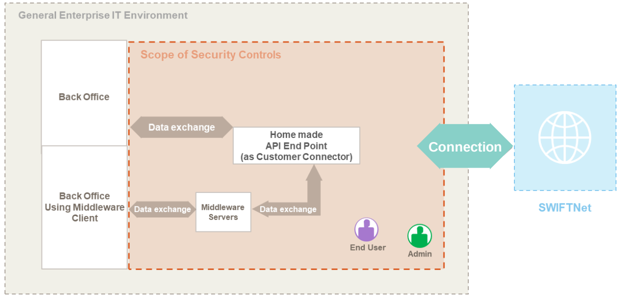
To facilitate app-to-app and to connect to Service Provider

- Reached through local software such as:
  - File Transfer solutions
  - MQ servers

A4


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

A4

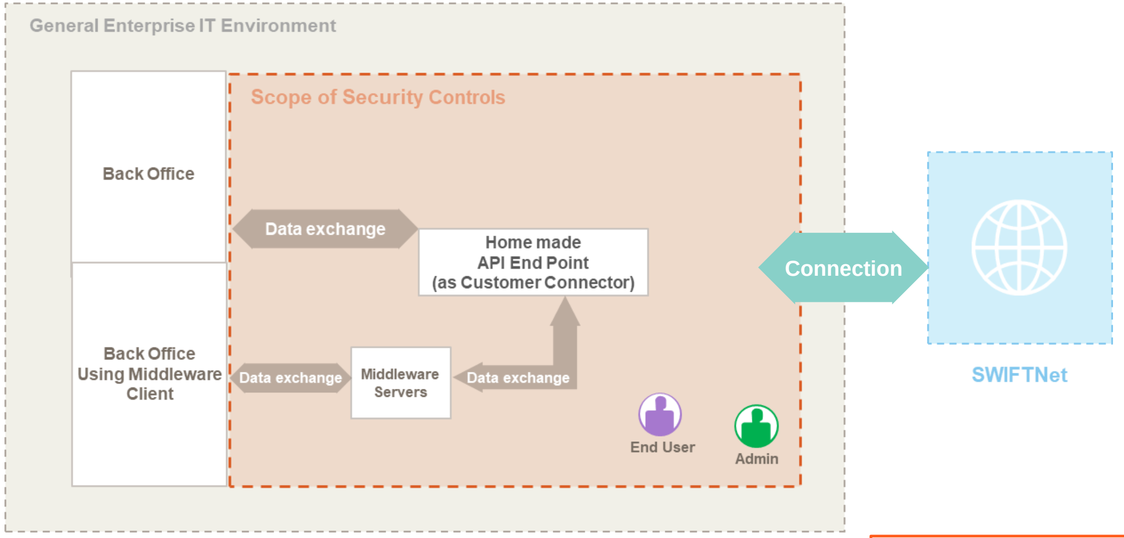

General Enterprise IT Environment
Scope of Security Controls
Back Office
Back Office Using Middleware Client
Data exchange
Home made API End Point (as Customer Connector)
Connection
Data exchange
Middleware Servers
Data exchange
End User
Admin
SWIFTNet

API introduction for app-to-app to connect to SWIFT services like

- Alliance Cloud, Lite2 or (future) messaging service or Transaction Platform exposed by SWIFT (and accessible through APIs)

CSCF v2021 | Focus on A4 with Customer “Home made* API” Connector

User Environment (Architecture A4 with local footprint)


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

Limited set of applicable controls for A4:

- Basic Security Hygiene controls
- Connectivity specific controls for App2app data exchange

And if U2A functionalities are present:

- GUI (end users) related controls

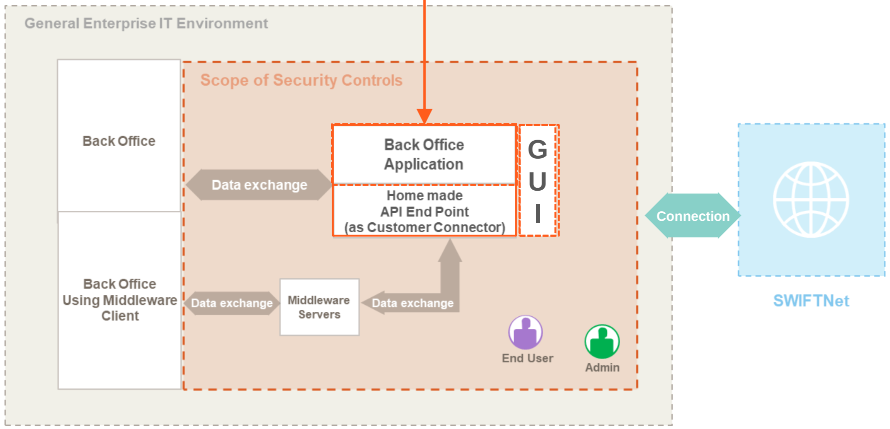
Back Office definition:

“Systems responsible for business logic, transaction generation, and other activities occurring before transmission.”

➔ In general Out of Scope

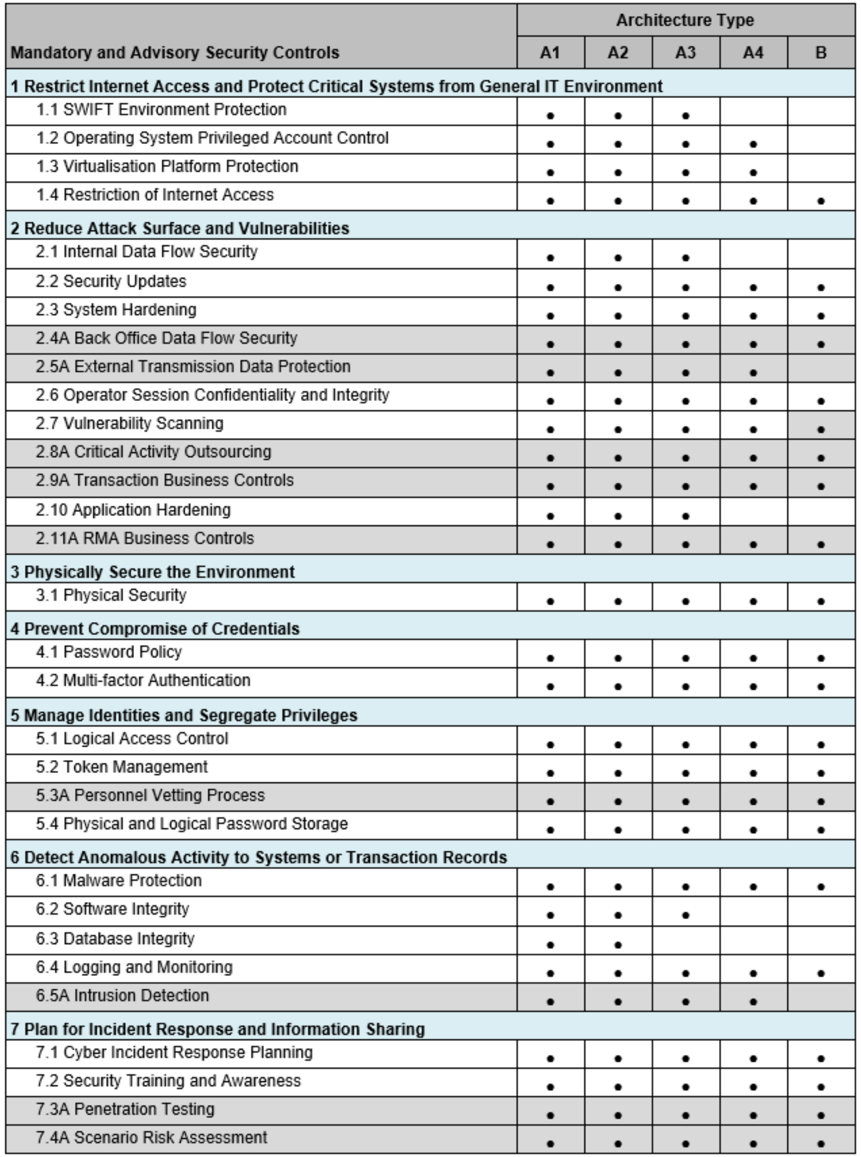
Pay attention:

If a **Back Office** application is **cohosted with** a Customer (Home made) Connector, the **hosting system** (and its accesses) **is in scope**.


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

* “Home made” = in-house build

CSCF v2021| Summary tables and controls applicability



	Architecture Type				
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	●	●	●	●	●

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

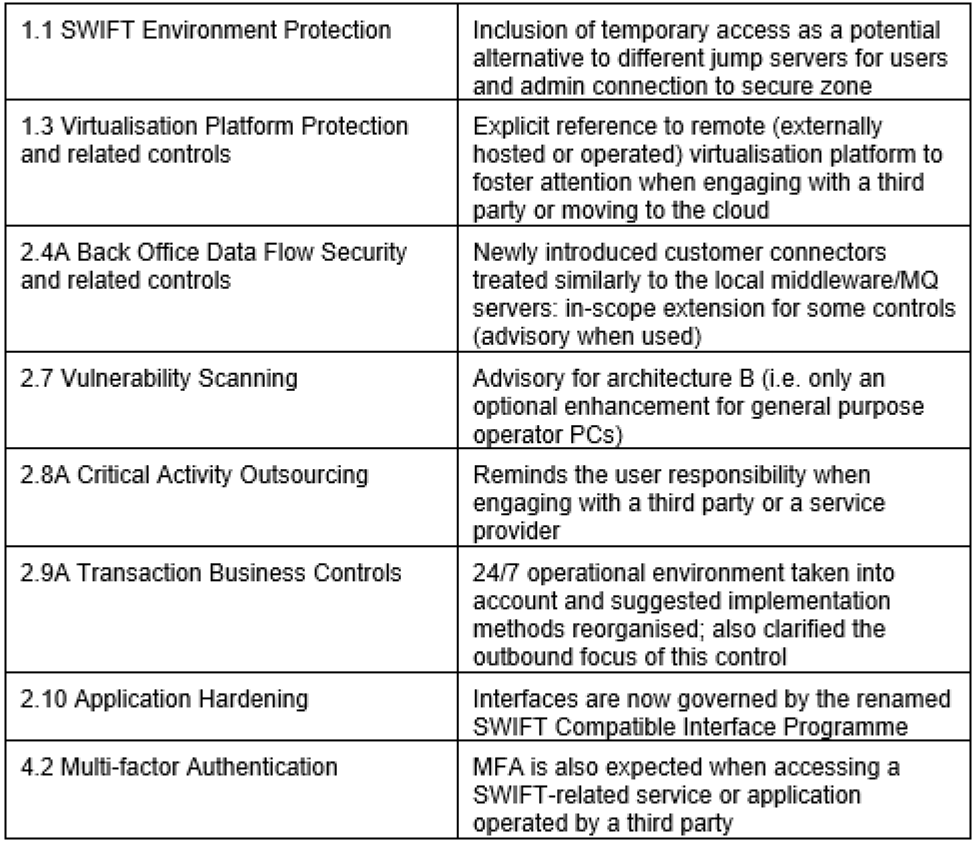
See also Annex F of the CSCF v2021 for controls applicability

CSCF v2021 | Key changes – part 2

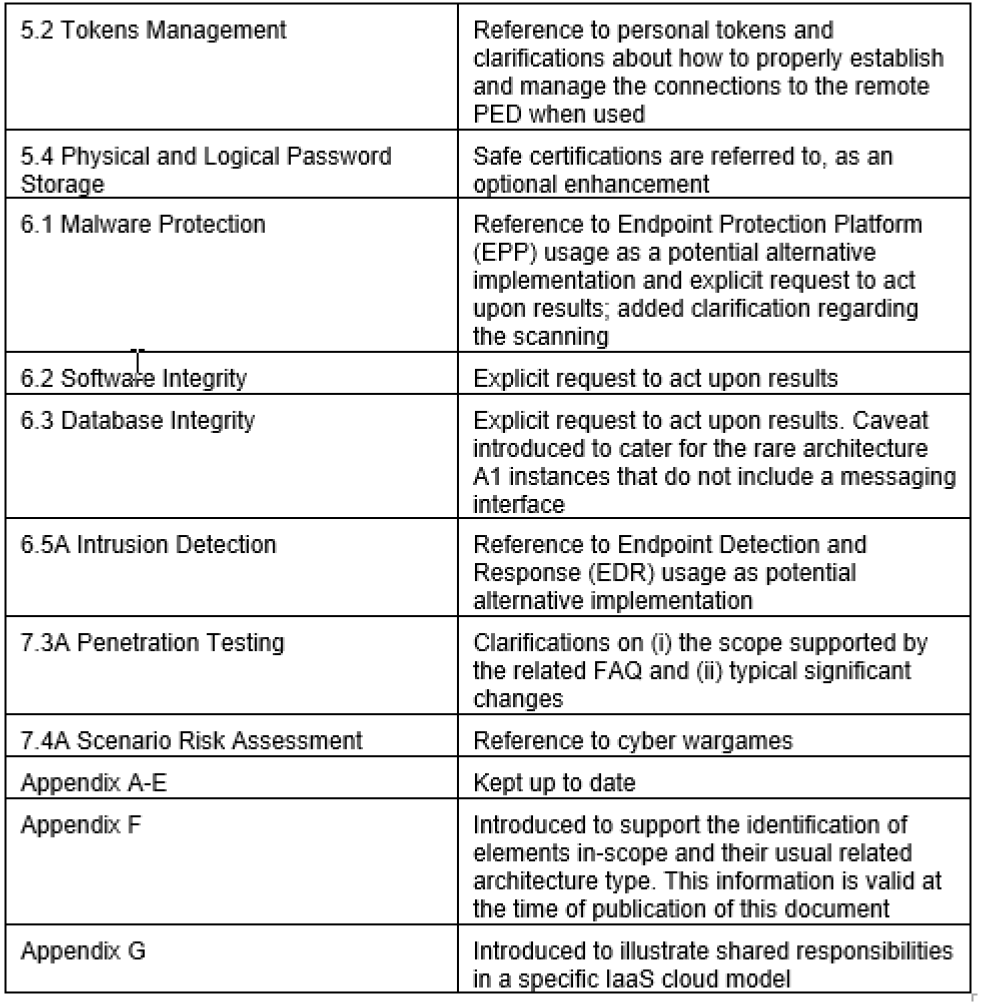
Clarifications – for Efficiency and Alignment to Reality

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

CSCF v2021 | Clarifications for efficiency and alignment to reality

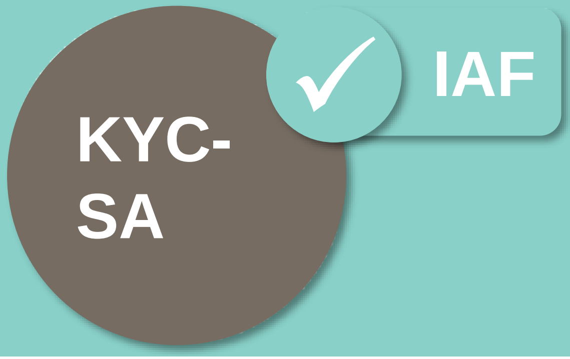


1.1 SWIFT Environment Protection	Inclusion of temporary access as a potential alternative to different jump servers for users and admin connection to secure zone
1.3 Virtualisation Platform Protection and related controls	Explicit reference to remote (externally hosted or operated) virtualisation platform 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)



KYC Security Attestation

Supporting Baseline 2021.1

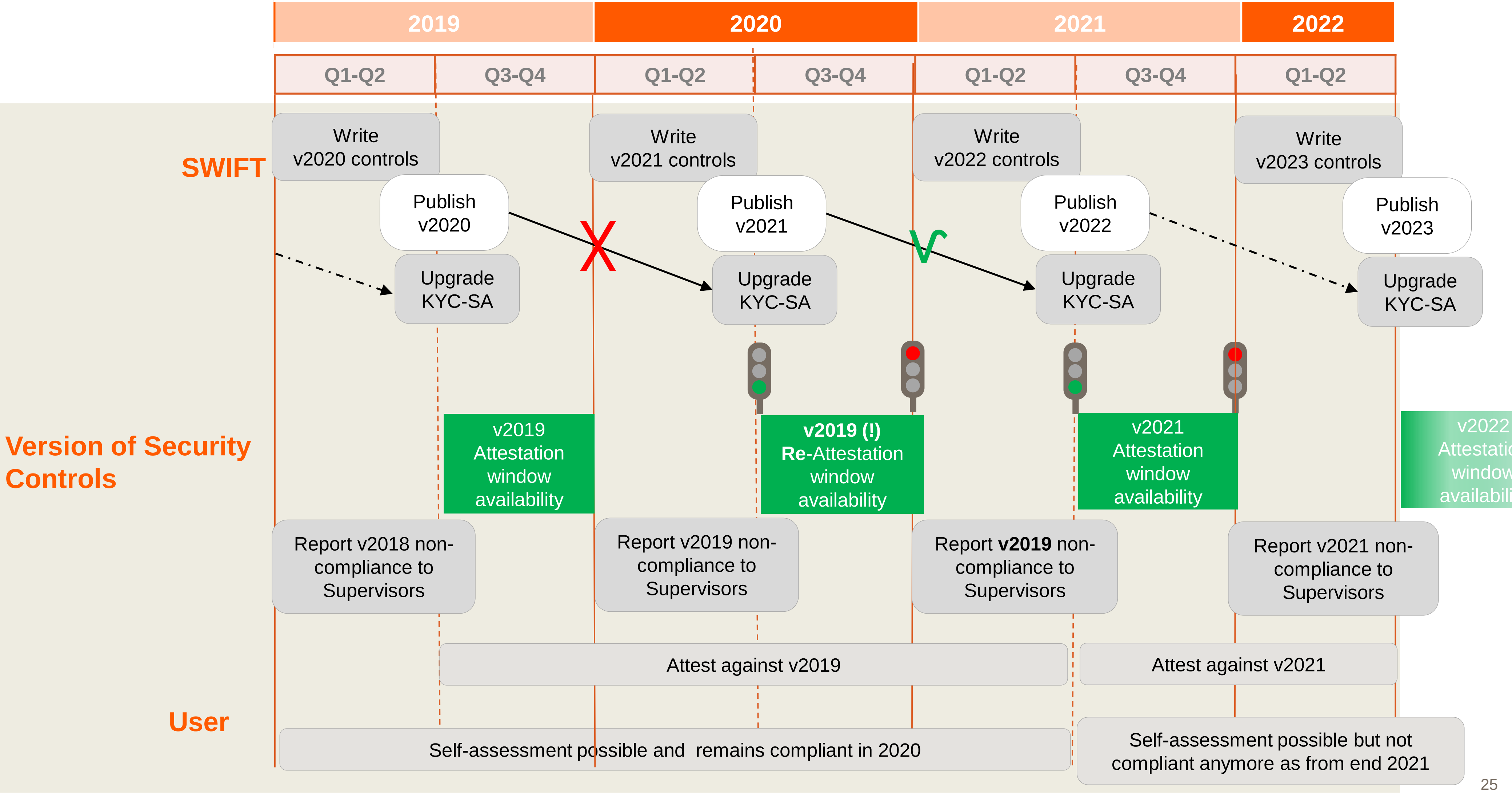
CSP | Flavours of the assessments

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

Note: it is preferable to attest using the self-assessment option than not to attest at all by December 2021

Start of IAF

CSP | Timeline



2019 | 2020 | 2021 | 2022

Q1-Q2 | Q3-Q4 | Q1-Q2 | Q3-Q4 | Q1-Q2 | Q3-Q4 | Q1-Q2

SWIFT

Write v2020 controls

Publish v2020

Upgrade KYC-SA

Write v2021 controls

Publish v2021

Upgrade KYC-SA

Write v2022 controls

Publish v2022

Upgrade KYC-SA

Write v2023 controls

Publish v2023

Upgrade KYC-SA

X

√

Version of Security Controls

v2019 Attestation window availability

v2019 (!) Re-Attestation window availability

v2021 Attestation window availability

v2022 Attestatio window availabili

Report v2018 non-compliance to Supervisors

Report v2019 non-compliance to Supervisors

Report **v2019** non-compliance to Supervisors

Report v2021 non-compliance to Supervisors

Attest against v2019

Attest against v2021

User

Self-assessment possible and remains compliant in 2020

Self-assessment possible but not compliant anymore as from end 2021

IAF | How do I keep costs under control?

- **An assessment**, not an audit is required
- Ensure an **accurate scope**:
  - Identify the correct architecture type
  - Only consider in scope components
  - Apply sampling of components wisely
- Consider **internal** vs external resources or even mixed team. Consider switching between internal and external resources
- Compare assessors quotes
- Leverage **previous** relevant and current (i.e. not older than 2 years) assessment results/documents
- Consider **automated** compliance reporting and/or **continuous** monitoring
- Consider quoting and engaging with one of your **service providers** (SIP/L2BA) to conduct the assessment

IAF | Assessment Vs Audit

The objective is the same: providing comfort or assurance on the compliance with the stated CSCF Control **Definition**.'

Where, in the CSCF, the Control Definition = Control Objective + In-scope Components + Risk Drivers

- The two approaches (Assessment / Audit) are possible:
  - **Assessments** are more **flexible,** not too deep 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 comfort is provided (assessment or audit) provided the firm (and the individual assessors) possess the necessary skills and certification as set out in the independent Assessment Framework.

IAF | Internal vs External assessors

Customers are free to select **internal** or **external** resources to conduct the assessment:

- As for internal resources, customers must ensure that:
  - The assessment team is **independent** from the 1st line of defence (CISO): eligible teams are typically Internal Audit (3d line of defence), Risk Office (2nd line of defence) or a tailored independent team established for the assessment.
  - The assessment team members have the appropriate **expertise, assessment skills and credentials.**
- Any external resources **may** be selected from the CSP assessment providers list on swift.com.

IMPORTANT

- An option can also be to appoint a **mixed team of internal/external professionals** lead by an internal or external staff. Such set up can enable cross expertise breeding and costs containments for subsequent assessments.
- All options i.e. Internal, external assessor or mixed team are **equally valid** for SWIFT
- The lead assessor **MUST** hold at least one industry-relevant professional certification and other individuals could hold similar certification. SWIFT expect a close oversight from the lead assessor on the activities performed by the other individuals members of the team

IAF | 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

IAF | Independent assessment Framework flow and timeline

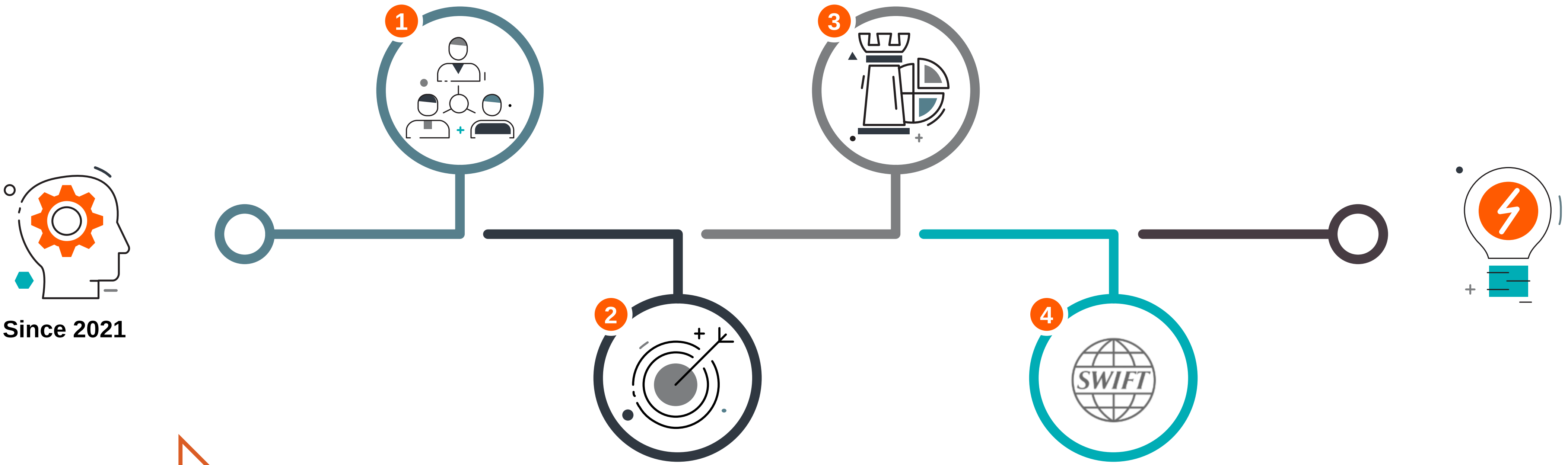
Independent assessor selection

- 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 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 2021

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 compliant attestation and swift reserves the right for reporting to the local supervisors and visible to counterparties via the KYC-SA application
- **An independent assessment will have a validity period of maximum two years under conditions**

IAF | Resources available to CSP assessors

CSCF and IAF documentation (translations available)

CSP curriculum (Annex A of the IAF - PDF)

Security Guidance covering SWIFT Products suite

Excel-based Assessment Templates and Word Completion letter

SWIFTSmart (IAF, Policy, CSCF)

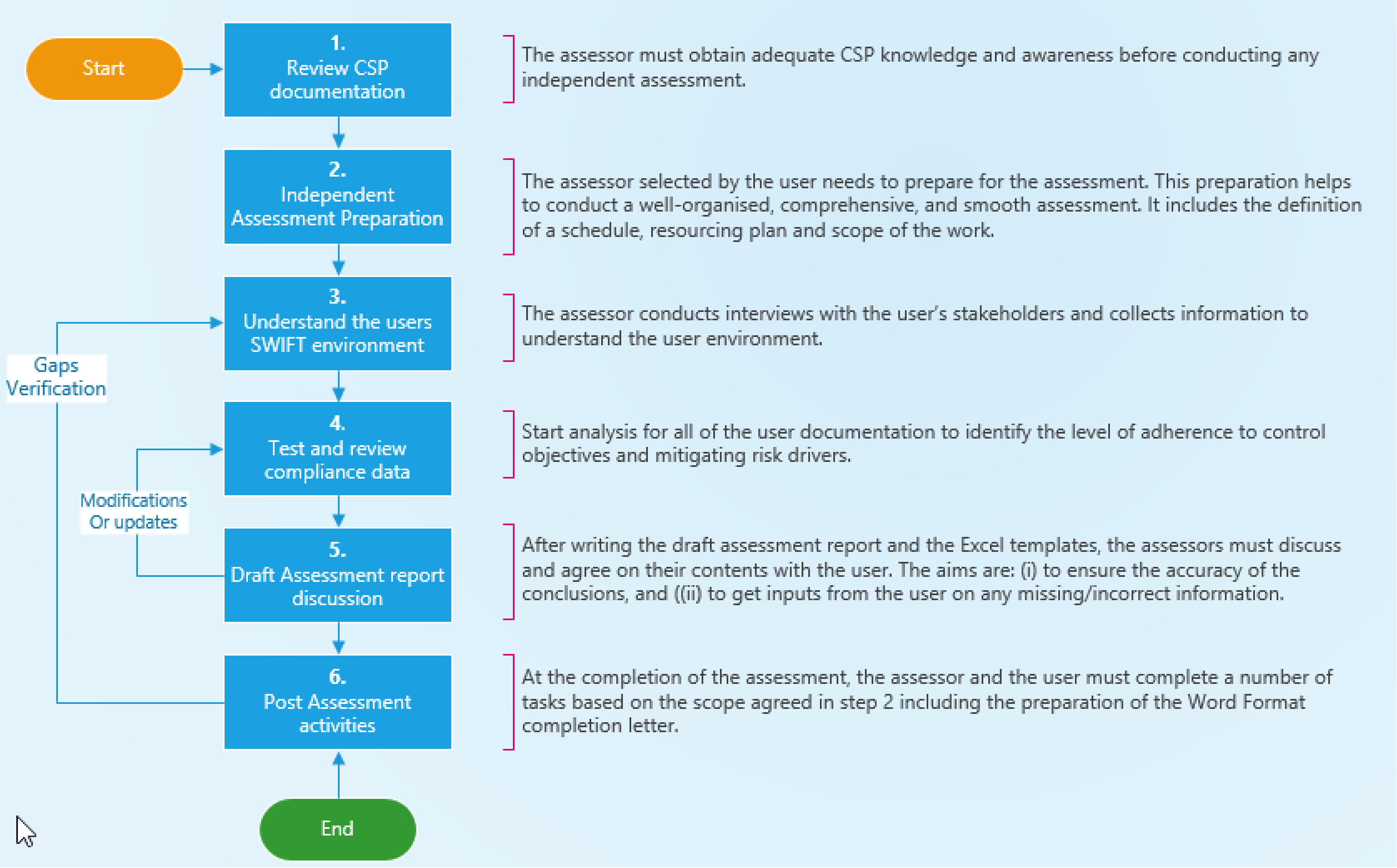
Independent Assessment Process guidelines

New in 2021

High Level test plan guidance (v2021)

New in 2021

IAF | Independent Assessment Process - Guidance



Start

Gaps Verification

Modifications Or updates

End

Process Step	Objective
1. Review CSP documentation	The assessor must obtain adequate CSP knowledge and awareness before conducting any independent assessment.
2. Independent Assessment Preparation	The assessor selected by the user needs to prepare for the assessment. This preparation helps to conduct a well-organised, comprehensive, and smooth assessment. It includes the definition of a schedule, resourcing plan and scope of the work.
3. Understand the users SWIFT environment	The assessor conducts interviews with the user's stakeholders and collects information to understand the user environment.
4. Test and review compliance data	Start analysis for all of the user documentation to identify the level of adherence to control objectives and mitigating risk drivers.
5. Draft Assessment report discussion	After writing the draft assessment report and the Excel templates, the assessors must discuss and agree on their contents with the user. The aims are: (i) to ensure the accuracy of the conclusions, and ((ii) to get inputs from the user on any missing/incorrect information.
6. Post Assessment activities	At the completion of the assessment, the assessor and the user must complete a number of tasks based on the scope agreed in step 2 including the preparation of the Word Format completion letter.

IAF | Independent assessment Framework – details (1/2)

Community-Standard Assessments

All customers from 2021

Internal or external assessment

Skilled Assessors

- **Independency**: as defined by ‘Institute of Internal Auditors’ (IIA)
- **Recent (12 months) and relevant experience**, e.g. PCI DSS, ISO 27001
- **Qualifications**, The lead assessor **MUST** hold at least one industry-relevant professional certification and other individuals could hold similar certification. In any case, SWIFT expect a close oversight from the lead assessor on the activities performed by the other individuals members of the assessment team**.** 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 or PCI directory**
- **Service providers** such as service bureaus or L2BA are **eligible** under some conditions (*)
- SWIFT **does not endorse or validate** any particular assessor

(*) as documented in chapter 9.1 of the IAF

IAF | Independent assessment 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 definition) • A **mix of assessment methods** as appropriate, e.g. interview, replay, documentation • Possible **leverage** of **existing relevant assessment**
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/evidence in line with local legislation
Escalation	• **Absence** of assessment results in potential **reporting to the supervisors** and visibility to counterparties
Costs	• **Customer** is **responsible** for **costs** associated with the assessment

IAF | Options for remote assessments

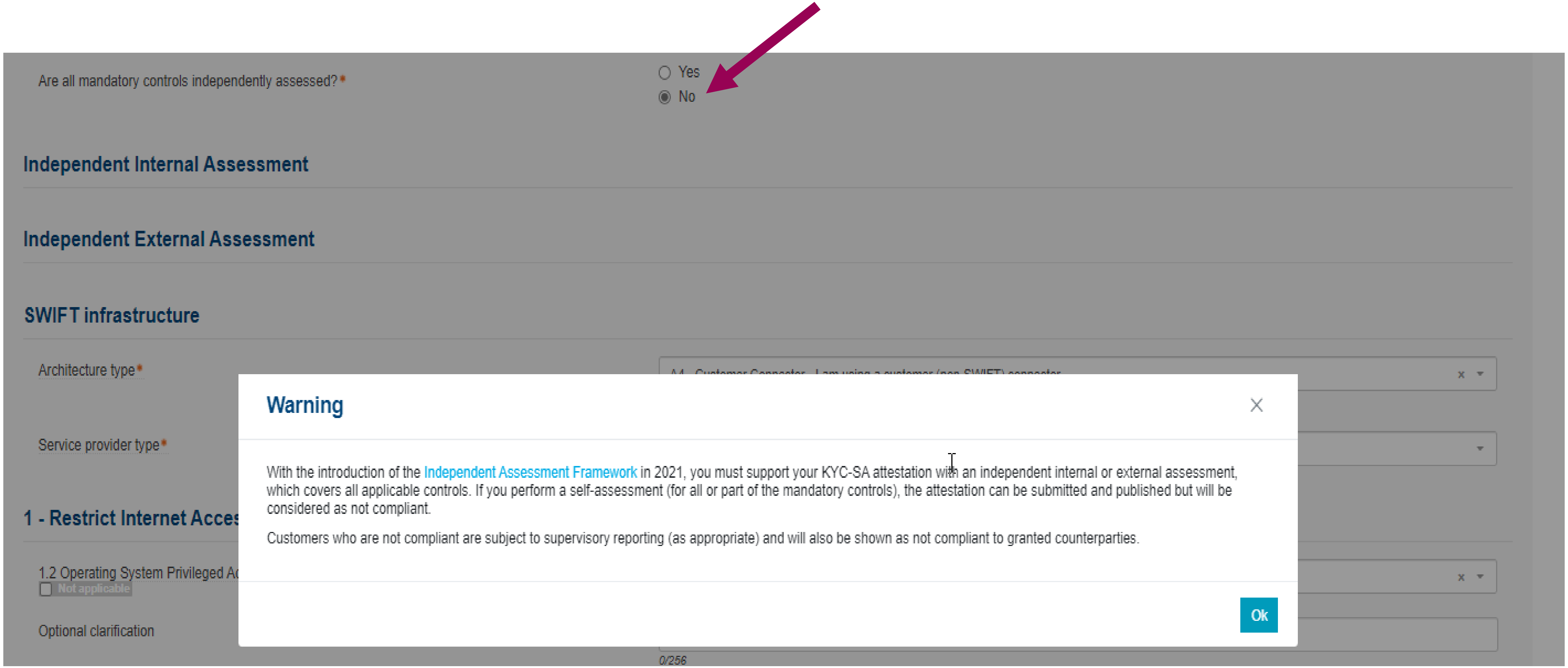
The covid-19 pandemic may limit assessors' and customers' abilities to travel and conduct on-site assessments; options to conduct an adequate assessment **remotely** are:

- For technical and organizational controls, assessors can rely on the **review of documentation**:
  - Screenshots (for example, network diagrams)
  - System extracts/procedures complemented by remote staff interviews

- For physical controls, assessors can **combine** the review of documentation (for example, maps or schemas) with interviews and images or video recordings

Demo-
IAF and KYC-SA Attestation Portal

Selecting Self Assessment is considered as not Compliant as of 2022



Are all mandatory controls independently assessed?*

○ Yes
● No

Independent Internal Assessment

Independent External Assessment

SWIFT infrastructure

Architecture type* A4 - Customer Connector - I am using a customer (non SWIFT) connector

Service provider type*

1 - Restrict Internet Acces

1.2 Operating System Privileged Ac

□ Not applicable

Optional clarification

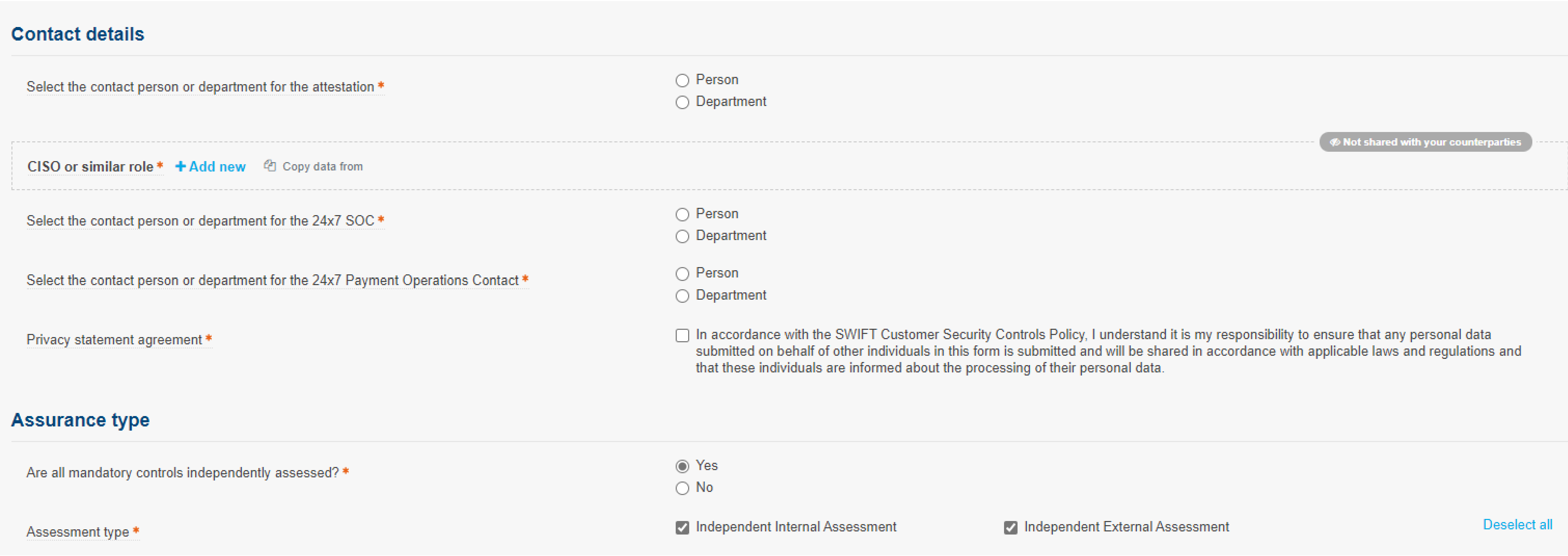
0/256

Warning

With the introduction of the Independent Assessment Framework in 2021, you must support your KYC-SA attestation with an independent internal or external assessment, which covers all applicable controls. If you perform a self-assessment (for all or part of the mandatory controls), the attestation can be submitted and published but will be considered as not compliant.

Customers who are not compliant are subject to supervisory reporting (as appropriate) and will also be shown as not compliant to granted counterparties.

Selecting Internal/external assessors



Contact details

Select the contact person or department for the attestation *
○ Person
○ Department

Not shared with your counterparties

CISO or similar role * + Add new Copy data from

Select the contact person or department for the 24x7 SOC *
○ Person
○ Department

Select the contact person or department for the 24x7 Payment Operations Contact *
○ Person
○ Department

Privacy statement agreement *
□ In accordance with the SWIFT Customer Security Controls Policy, I understand it is my responsibility to ensure that any personal data submitted on behalf of other individuals in this form is submitted and will be shared in accordance with applicable laws and regulations and that these individuals are informed about the processing of their personal data.

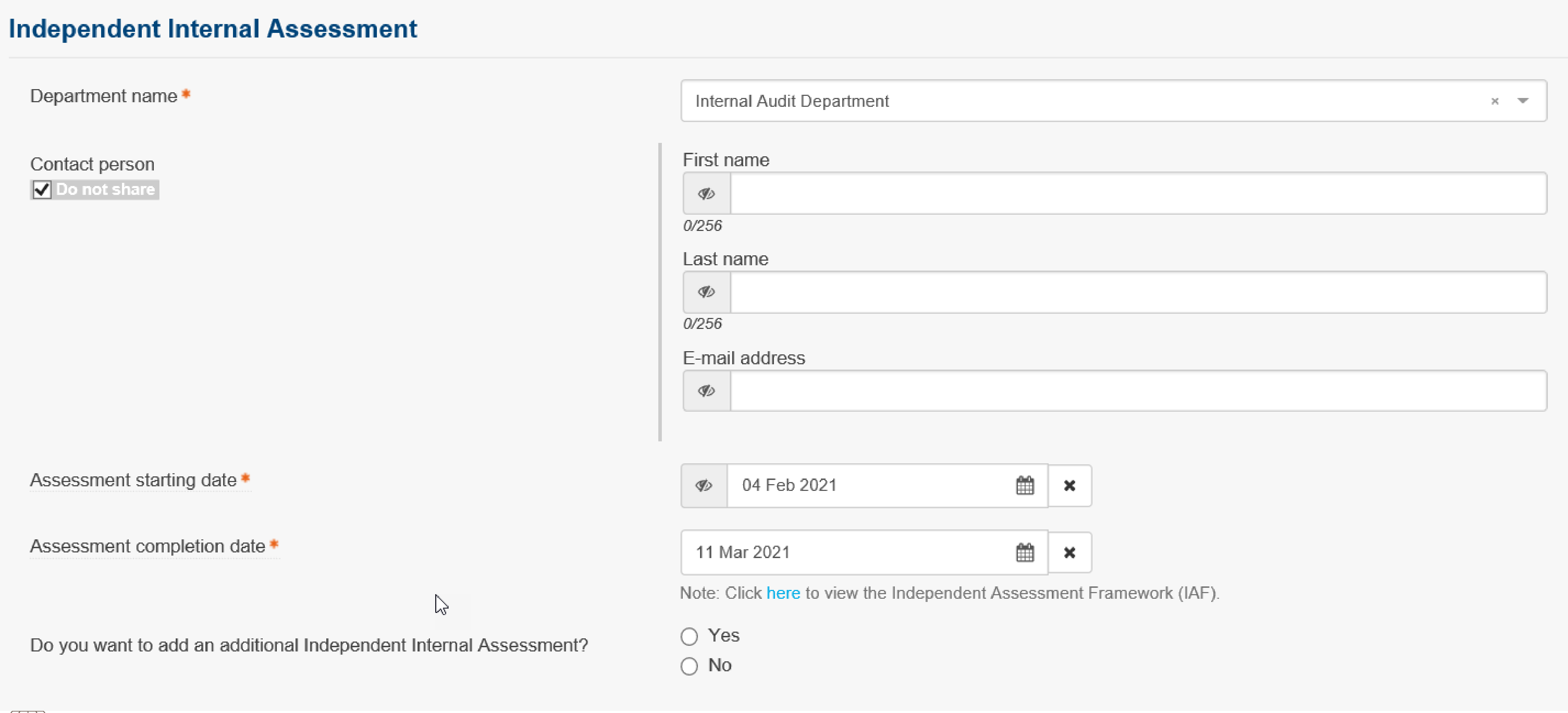
Assurance type

Are all mandatory controls independently assessed? *
● Yes
○ No

Assessment type *
☑ Independent Internal Assessment ☑ Independent External Assessment

Deselect all

Data requested for Internal Assessor



Independent Internal Assessment

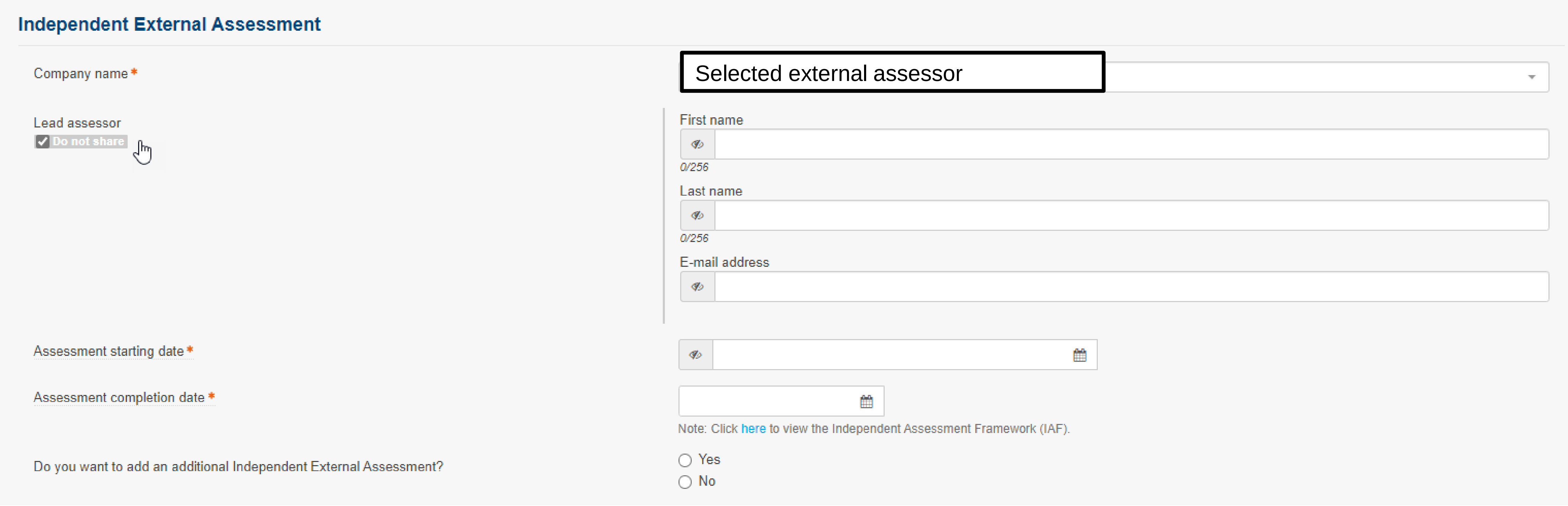
Department name *	Internal Audit Department
Contact person ☑ Do not share	First name 0/256 Last name 0/256 E-mail address
Assessment starting date *	04 Feb 2021
Assessment completion date *	11 Mar 2021

Note: Click here to view the Independent Assessment Framework (IAF).

Do you want to add an additional Independent Internal Assessment?

○ Yes
○ No

Data requested for External Assessor



Independent External Assessment

Company name *

Selected external assessor

Lead assessor

☑ Do not share

First name

0/256

Last name

0/256

E-mail address

Assessment starting date *

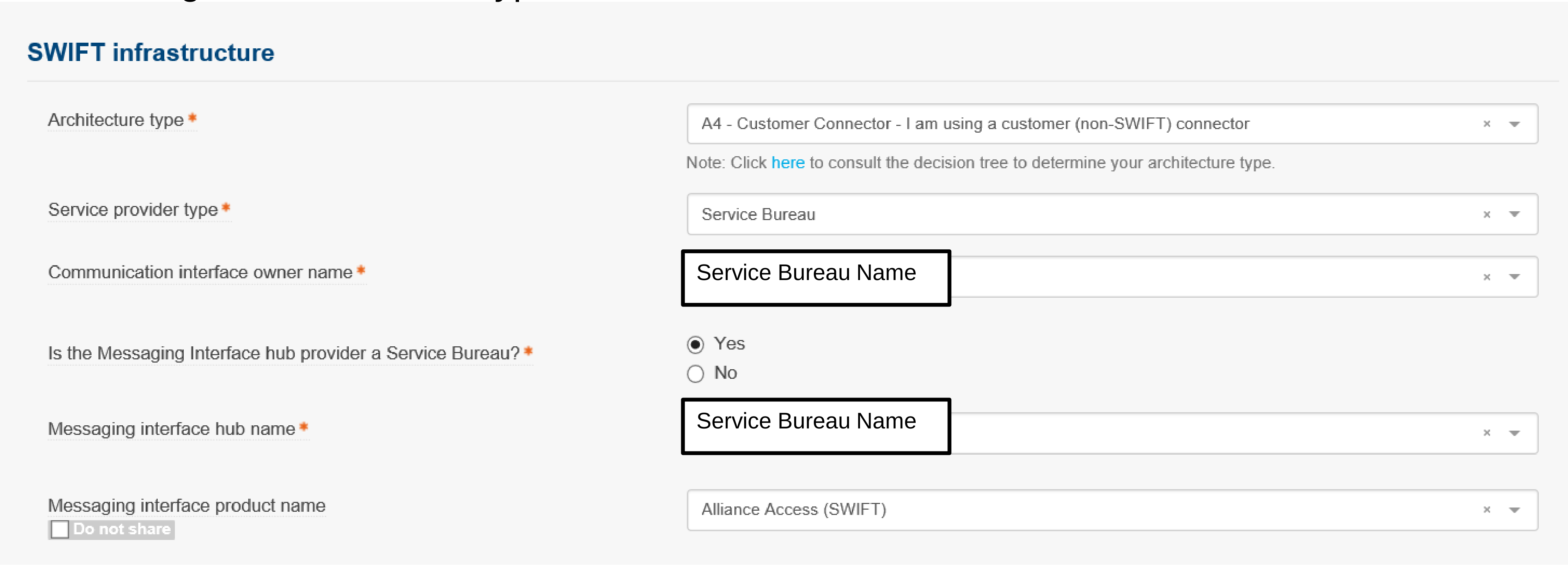
Assessment completion date *

Note: Click here to view the Independent Assessment Framework (IAF).

Do you want to add an additional Independent External Assessment?

○ Yes
○ No

Selecting A4 Architecture Type



SWIFT infrastructure

Architecture type *	A4 - Customer Connector - I am using a customer (non-SWIFT) connector × ▾ Note: Click here to consult the decision tree to determine your architecture type.
Service provider type *	Service Bureau × ▾
Communication interface owner name *	Service Bureau Name × ▾
Is the Messaging Interface hub provider a Service Bureau? *	● Yes ○ No
Messaging interface hub name *	Service Bureau Name × ▾
Messaging interface product name □ Do not share	Alliance Access (SWIFT) × ▾

Highlights of the Customer Security Control Framework v2022

CSP | CSCF v2022 Changes

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**

F
A
Q

CSP | FAQ

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

I already submitted an attestation in 2021, do I have to re-attest in 2021?

Can I reuse an independent Assessment I did last year ?

Do I need to cover advisory controls in my independent assessment to be considered as compliant ?

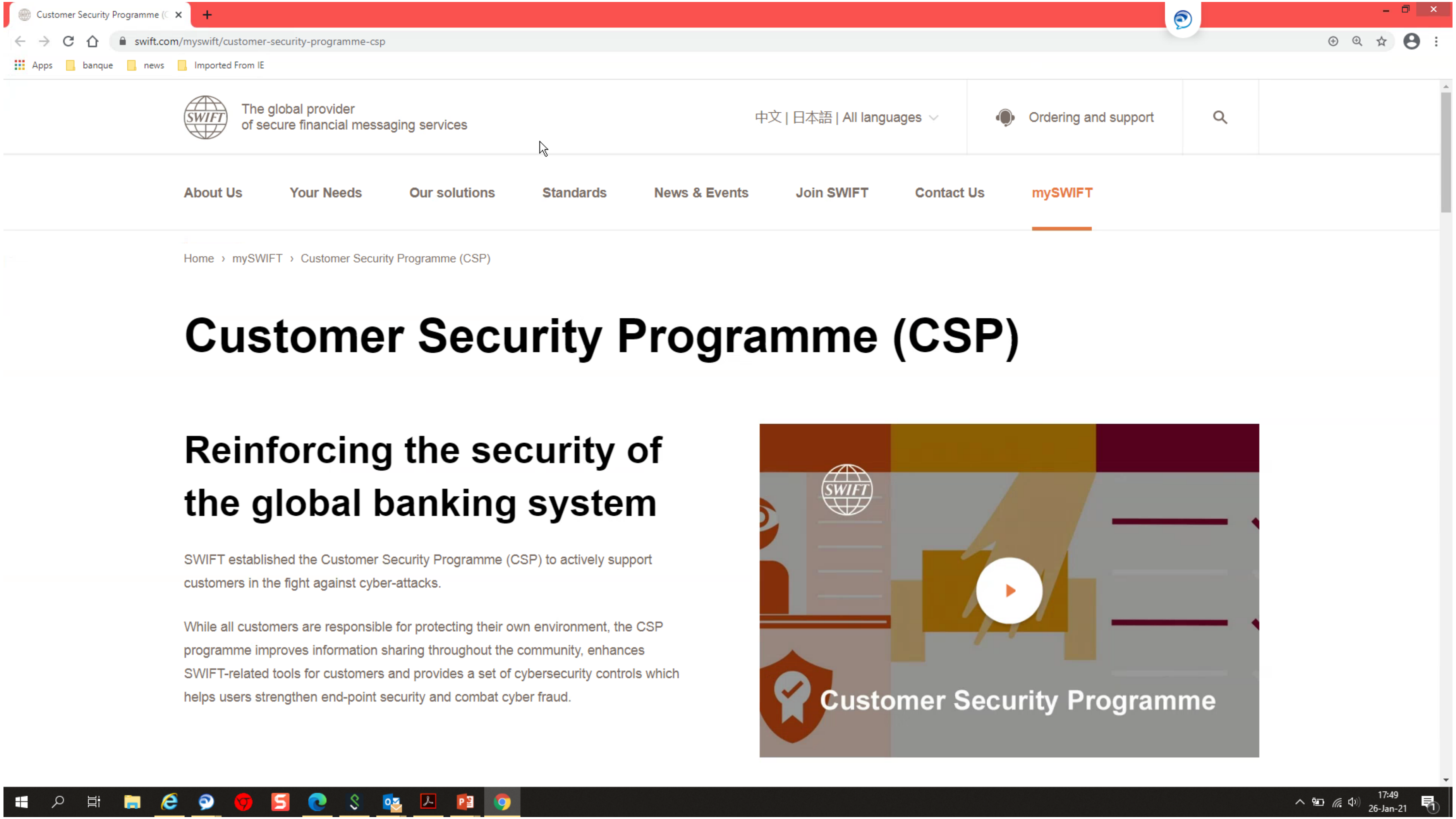
What is the impact on my compliance if the service bureau / l2ba that serves me is delisted ?

What are the consequences if am not compliant ?

Questions

How SWIFT can help

CSP | Supporting the Community – **swift.com/csp** one stop hub for all CSP Information


Customer Security Programme (C
swift.com/myswift/customer-security-programme-csp
Apps
banque
news
Imported From IE
The global provider
of secure financial messaging services
中文 | 日本語 | All languages
Ordering and support
About Us
Your Needs
Our solutions
Standards
News & Events
Join SWIFT
Contact Us
mySWIFT
Customer Security Programme
17:49
26-Jan-21

Home › mySWIFT › Customer Security Programme (CSP)

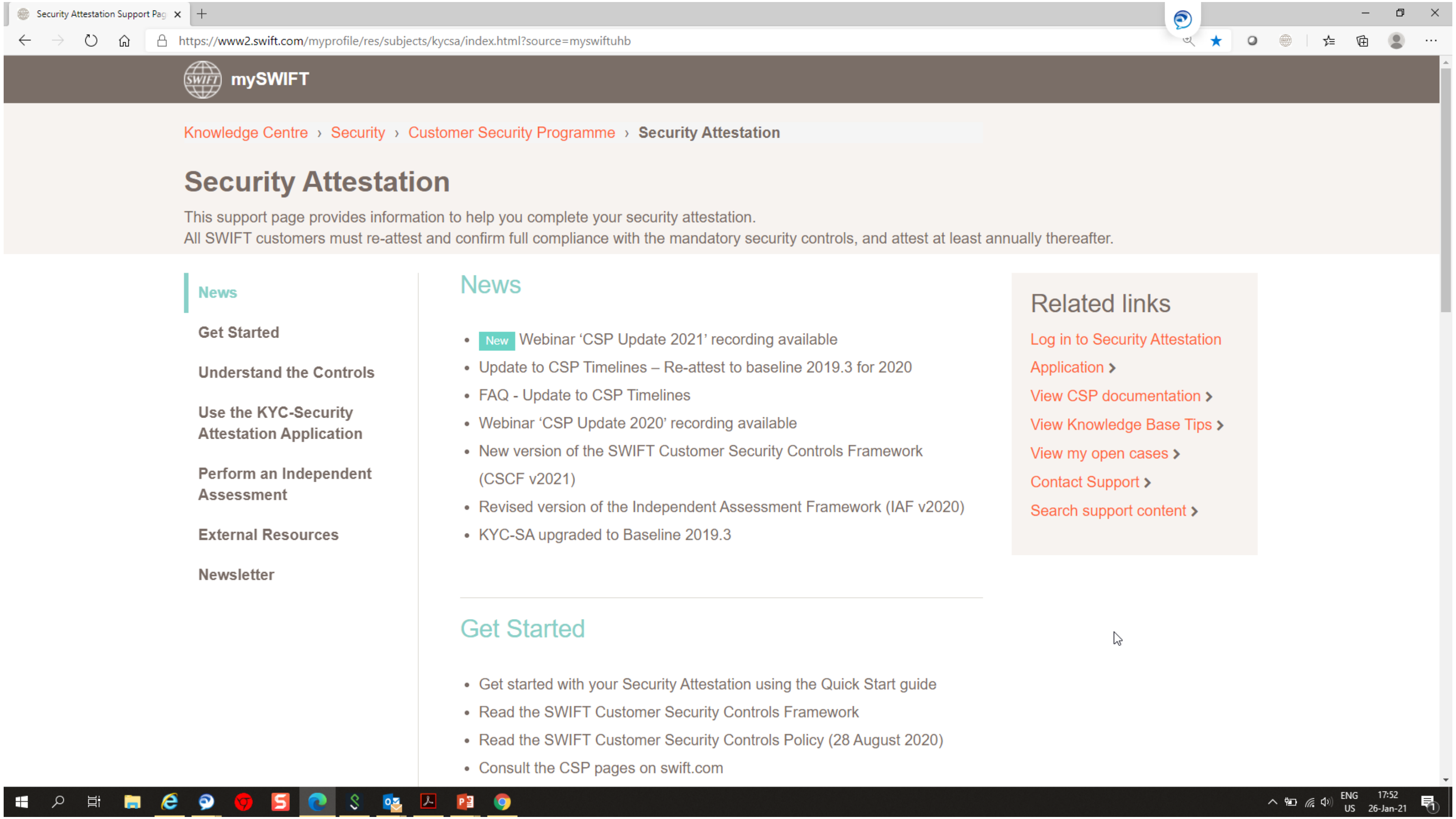
Customer Security Programme (CSP)

Reinforcing the security of the global banking system

SWIFT established the Customer Security Programme (CSP) to actively support customers in the fight against cyber-attacks.

While all customers are responsible for protecting their own environment, the CSP programme improves information sharing throughout the community, enhances SWIFT-related tools for customers and provides a set of cybersecurity controls which helps users strengthen end-point security and combat cyber fraud.

CSP | Supporting the Community – one stop hub for all KYC-SA Information


Security Attestation Support Pag
https://www2.swift.com/myprofile/res/subjects/kycsa/index.html?source=myswiftuhb
mySWIFT

Knowledge Centre › Security › Customer Security Programme › Security Attestation

Security Attestation

This support page provides information to help you complete your security attestation.
All SWIFT customers must re-attest and confirm full compliance with the mandatory security controls, and attest at least annually thereafter.

- News
- Get Started
- Understand the Controls
- Use the KYC-Security Attestation Application
- Perform an Independent Assessment
- External Resources
- Newsletter

News

- New Webinar 'CSP Update 2021' recording available
- Update to CSP Timelines – Re-attest to baseline 2019.3 for 2020
- FAQ - Update to CSP Timelines
- Webinar 'CSP Update 2020' recording available
- New version of the SWIFT Customer Security Controls Framework (CSCF v2021)
- Revised version of the Independent Assessment Framework (IAF v2020)
- KYC-SA upgraded to Baseline 2019.3

Related links

- Log in to Security Attestation Application ›
- View CSP documentation ›
- View Knowledge Base Tips ›
- View my open cases ›
- Contact Support ›
- Search support content ›

Get Started

- Get started with your Security Attestation using the Quick Start guide
- Read the SWIFT Customer Security Controls Framework
- Read the SWIFT Customer Security Controls Policy (28 August 2020)
- Consult the CSP pages on swift.com

CSP | Supporting the Community – CSP Directories

Directory of CSP Assessment Providers

If you need assistance from a third party to perform the Independent **assessment**, consult the Directory of CSP assessment:

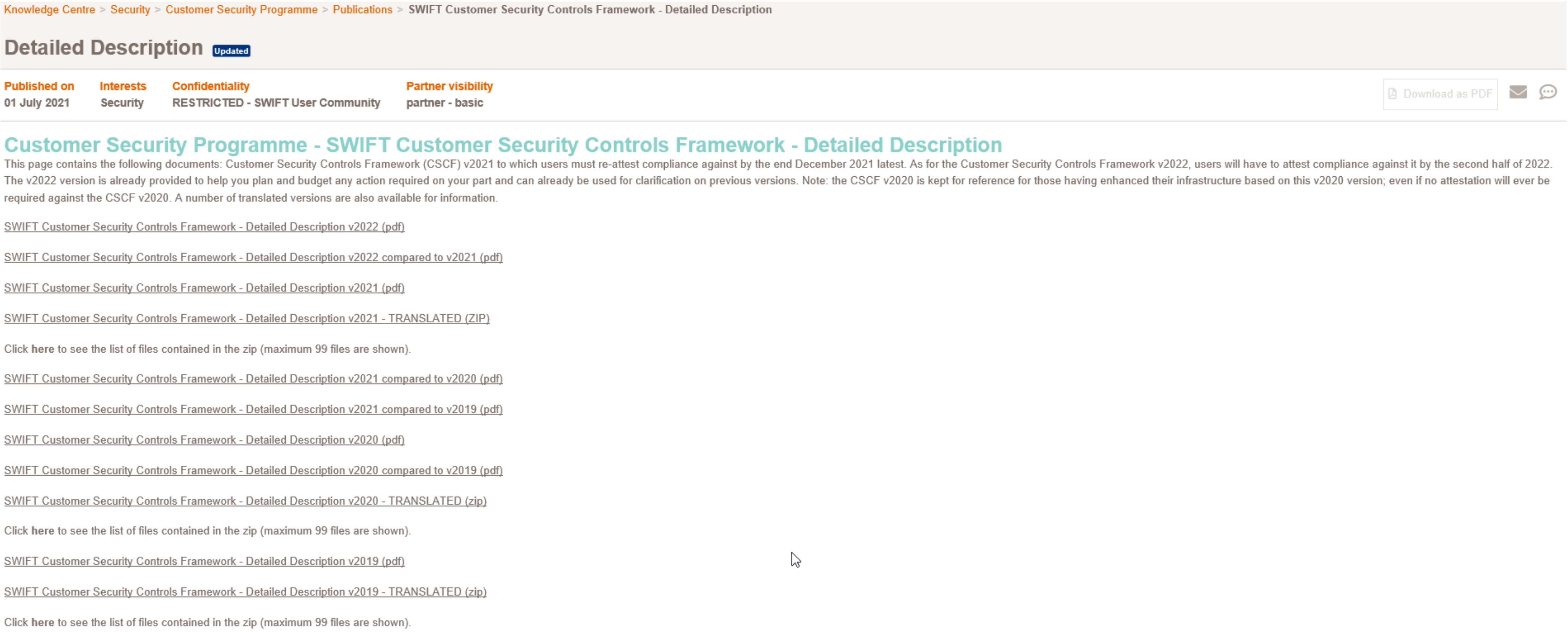
- Non prescriptive list
- Basic due diligence performed by SWIFT
- Requires passing of SWIFTSmart quiz
- Not certified by SWIFT

Directory of Cyber Security Service Providers

If you need practical, on-the-ground **implementation support and advice**, you can consult the Directory of Cyber Security Service Providers on SWIFT.com

- Non prescriptive list
- Basic due diligence performed by SWIFT
- Requires passing of SWIFTSmart quiz
- Not certified by SWIFT

CSP | Supporting the Community – Knowledge center



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

Detailed Description Updated

Published on 01 July 2021

Interests Security

Confidentiality RESTRICTED - SWIFT User Community

Partner visibility partner - basic

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

This page contains the following documents: Customer Security Controls Framework (CSCF) v2021 to which users must re-attest compliance against by the end December 2021 latest. As for the Customer Security Controls Framework v2022, users will have to attest compliance against it by the second half of 2022. The v2022 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 v2022 (pdf)

SWIFT Customer Security Controls Framework - Detailed Description v2022 compared to v2021 (pdf)

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

SWIFT Customer Security Controls Framework - Detailed Description v2021 - 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 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 - summary

swift.com*

* Login required

Security Attestation support home page

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
- Decision Tree 2022

Knowledge Base

- Tip 5021823: CSP FAQ
- Tip 5022902: IAF FAQ
- Tip 5020786 Security Guidance

SWIFT ISAC and MISP Portals

Consult the Portal / MISP 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.

There is also a module related to the IAF.

MySWIFT

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

Customer Security Programme

SWIFTSmart e-learning modules

Security and Audit

SWIFT Customer Security Controls Framework v2019

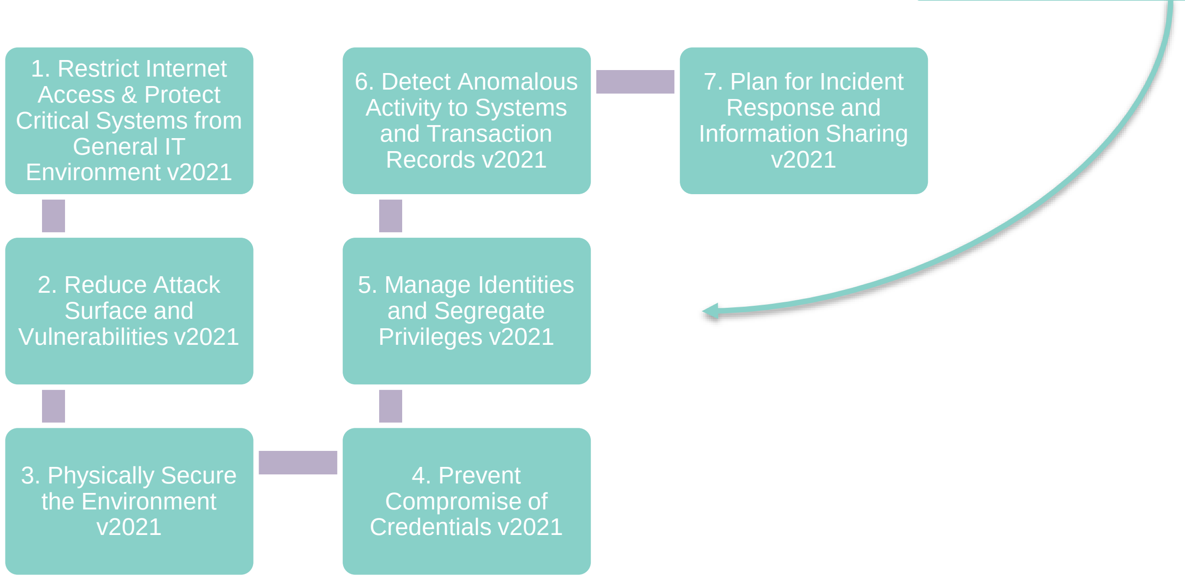
Security and Audit

SWIFT Customer Security Controls Framework v2020

Security and Audit

SWIFT Customer Security Controls Framework v2021

SWIFT Customer Security Controls Framework v2021


1. Restrict Internet Access & Protect Critical Systems from General IT Environment v2021

2. Reduce Attack Surfeace and Vulnerabilities v2021

3. Physically Secure the Environment v2021

4. Prevent Compromise of Credentials v2021

5. Manage Identities and Segregate Privileges v2021

6. Detect Anomalous Activity to Systems and Transaction Records v2021

7. Plan for Incident Response and Information Sharing v2021

Understand how to be compliant with SWIFT mandatory and advisory security controls, to reinforce the security of the SWIFT secure zone of your organisation.

This curriculum provides an introduction to the 22 mandatory security controls for SWIFT users. You are guided through each control based on your SWIFT architecture type and explained the most common risks that you can mitigate by complying with them. This learning path prepares you to implement the security guidelines provided in the SWIFT Customer Security Controls Framework document version 2021.From July 2021 until December 2021 you will need to attest against the combined control framework requirements for 2020 and 2021, supported by an independent assessment.

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.

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.

SWIFT

www.swift.com