

Raise the Security Bar – Scope change

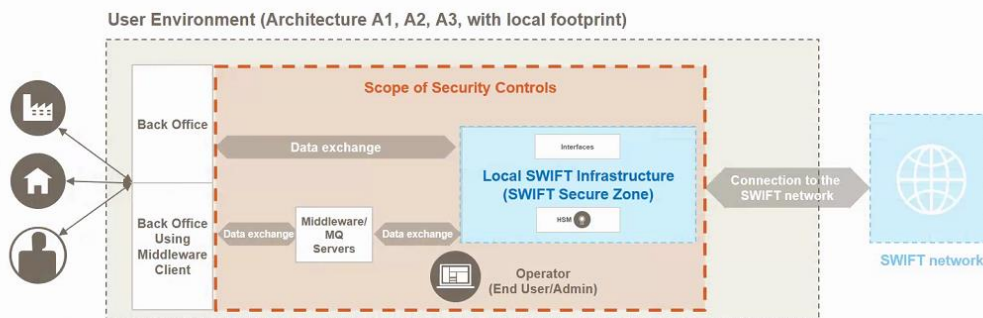
1. Introduced Architecture type A4
2. Fully transfer 'Internet Access' provisions from control 1.1 to 1.4 (Restrict Internet Access)

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	*	*	*	*	*



11

CSCF v2021 | CSP Scope in the CSCF v2020



Back Office definition:

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

→ In general Out of Scope



16

CSCF v2021 | Introduction of architecture A4 with CSCF v2021

Viewing Daniel MORAN...

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



A3

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

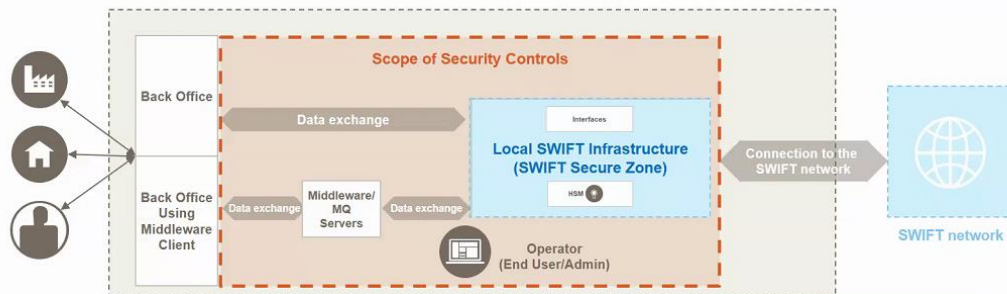
A4



19

CSCF v2021 | CSP Scope in the CSCF v2020

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



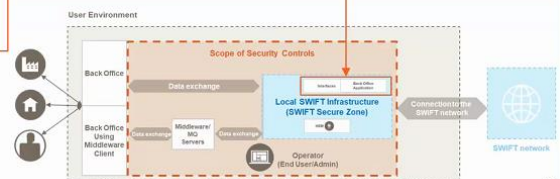
Back Office definition:

"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.



16

CSCF v2021 | Summary tables and controls applicability



Customer Security Programme

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 Identity 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



21

CSCF v2021 | Clarifications for efficiency and alignment to reality



Customer Security Programme

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



IAF | Independent Assessment Process - Guidance



33

CSP | Flavours of the assessments

Assessment Type	Selection Criteria	Assessor	Timeline			
			2019	2020	2021	2022 and beyond
<input type="checkbox"/> Self-Assessment	Still possible but will not be compliant after start of IAF	First Line of defense	Green	Green	Green	Not Compliant-reportable as of Jan 2022
<input type="checkbox"/> Community-Standard Assessment	Mandated for all customers with the start of IAF	Internal or external	Green	Green	Green	Green
<input type="checkbox"/> SWIFT-Mandated Assessment	Mandated - Sampled Customers Driven by QA Analysis	External only	Grey	Grey	Green	Green

Start of IAF



26

- 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**




44

File Edit View Audio & Video Participant Event Help

ALLEN LUM Me Daniel MORAN Host Megan SMITH Host Princy-joreh PILAZA Princ...

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.

Participants

Panelist: 3

- MS Megan S... Host
- DM Daniel MORAN
- PJ Princy-joreh PILAZA Princy joreh

Attendee:

- AL ALLEN LUM Me

Q & A

Unmute Share ...

Participants Chat ...