SWIFT Customer Security Controls Framework and KYC Security Attestation Application Frequently asked questions (FAQ) Updated

ID	Last update	Product & release	Change request	Found in	Fixed in
5021823	12 July 2021	Customer Security Programme	-	-	-

SWIFT Customer Security Controls Framework and KYC Security Attestation Application Frequently asked questions (FAQ)

Last revision

Date of revision	Section impacted	Details	Remark
12 July 2021	1.3 Virtualisation Platform Protection	How do I attest if I don't have a virtualization platform?	

View full revision record

Introduction

This FAQ aims at providing more in depth responses to questions raised on the controls documented by SWIFT in the SWIFT Customer Security Controls framework. (Please use v2021, to which customers have to comply by the end of December 2021).

The first section of this FAQ contains a set of generic questions that are applicable to the framework in general. The last section gathers questions and answers on the Attestation Policy & KYC Security Attestation Application.

To search for content within this tip, use the links in the Index and the browser's search. *Press **Ctrl+F** and type the text that you are looking for. Press **Enter**.*

© 2021 SWIFT

Generic information

Useful documents and links (swift.com login is required)

KYC-SA

CSCF

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

© 2021 SWIFT

- **CSP Pages**
  - Visit the CSP pages for programme news and updates.
  - Filter the Latest news with “Customer Security Programme” and/or “Cyber Security” for relevant topics
- **Knowledge Centre**
  - Access all the CSP docs (including IAF)
  - Access all the CSCF documents
  - Access some additional supporting documents and modules
  - SWIFT Customer Security Controls Policy
  - Customer Testing Policy
  - General Terms and Conditions
- **Knowledge Base**
  - Tip 5021823 - IAF FAQ
  - Tip 5022902 - IAF FAQ COVID-19
  - Tip 5024006 - FAQ - Update to CSP timelines
  - Tip 5020786 - Security Guidance
  - Tip 5022086 - Determine your architecture type (Decision Tree)
  - Tip 5024040 - Components in scope of CSP
  - Tip 5021567 - Passwords and PIN Policy Principles
  - Tip 5020533 - SWIFT Software and Malware Protection
  - Tip 5021566 - Guidance and Best Practices for Cryptography
  - Tip 2224150 - Known Operating System and third-party product incompatibilities
  - Tip 1212959 - Can you install SWIFT products on Operating System or third-party software versions that are different from those on which they have been qualified?
  - Tip 5021947 - KYC-SA welcome mail
- **SWIFTSmart**
  - The SWIFTSmart e-learning training platform includes a portfolio of modules, including in-depth modules on each of the mandatory security controls and includes a module related to the IAF
  - Tip 5021828 - KYC-SA Data Consultation
- **SWIFT ISAC Portal**
  - Consult the ISAC Portal for information related to security threats
- **MySWIFT**
  - A self-service portal containing “how-to” videos, guidance on frequently asked questions and Knowledge Base tips
  - Change your Legal or Publication information (e-form)
- **Directories of third party service providers**
  - Directory of Cyber Security Service Providers
  - Directory of CSP Assessment Providers

Back to Index

© 2021 SWIFT

Due to COVID-19, some SWIFT users/administrators in the organization will be required to work from home. As per CSP, what are the considerations to be taken into account?
A: Given current Covid-19 situation, many organisations are faced with the need for staff to work remotely, and also challenged with limited staffing due to lock-down restrictions to contain the pandemic. We want to assure you that the SWIFT's Security Control Framework (CSCF) continues to support the security of your organizations and your infrastructure during these crisis times.

To ensure organizations have proper business continuity plans, CSP continues to be applicable. As a rule - all controls that apply to General Operator PC remain relevant when accessing remotely. The following controls are most applicable to secure remote access during the pandemic situation:

- The control 1.1, section d.2 Remote Operator Access (teleworking, "on-call" duties, or remote administration) on page 21 of the CSCF.
- The control 3.1, Physical security: Security for Remote Workers (for example, teleworkers, "on call" operations staff) on page 49 of the CSCF.
- The control 4.2 on MFA on page 53 of the CSCF.

In addition, Cyber threats are likely to increase during this period, where hackers try to take advantage of the crisis using social engineering, spear phishing e-mails, and remote attacks. CSP continues to remain relevant to support the security of your organization while allowing your organisation to be Cyber resilient for business continuity, we encourage that each control is applied using a risk-based-approach and vigilance applied to prevent Cyber threats.

Can SWIFT recommend software/hardware for achieving on or more control objectives? Will SWIFT validate user compliance to security controls?
A: SWIFT does not provide recommendation for software/hardware or more generically product or technical solution for meeting controls objectives. In addition, SWIFT will not validate user's compliance with the security controls. Users are responsible for selecting any required software/hardware, product or technical solution that meets control objectives, based on assessment of their architecture type, design and configurations. After completion of implementation, users are responsible to complete attestations based on the status for each control. Users requiring specific support to assess, remediate and provide assurance against the security controls can engage a third party Cyber Security Service Provider.
As per Customer Security Policy, SWIFT also reserves the right to require users to deepen investigation or to seek additional independent assurance (for example, to conduct a SWIFT-Mandated external assessment) regarding the accuracy of their attestations and, as applicable, to correct their attestation accordingly.

How can an assessor confirm that I comply with a control? Do I need to implement SWIFT's implementaion guidelines to be compliant?
A: 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 an audit checklist.
Hence, the implementation of a CSP control can be:

- As per the documented SWIFT proposed Implementation Guidelines

© 2021 SWIFT

- An alternative Implementation that:
  - Meets the stated control objective, i.e. addresses the risk drivers
  - Covers the relevant in-scope components

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

Is there a document that we can reference that can help us to map the security controls of the framework to the functionality of SWIFT supplied software?
A: SWIFT provides a mapping between the security controls and the recommendations from SWIFT in the security guidance documents.
The mappings are available for:

- Alliance Access/Entry
- Alliance Messaging Hub
- Alliance Remote Gateway
- Alliance Lite2
- Alliance Gateway Instant
- Compatible interfaces by 3rd party providers

Users can find this information in the Knowledge Base Tip 5020786.

Do CSP controls apply to SWIFT Messaging and Communication Interfaces software only?
A: No, for each control there is a section called "In-scope components". The control must be applied on all the components in this section. These components can be SWIFT software, operator PCs, jump server, network devices, etc.

I am looking for help with meeting the controls, can SWIFT suggest a local consultant?
A: If you require specific local support to assess, remediate and provide assurance against the security controls, you can engage the support of a third-party Cyber Security Service Provider.
SWIFT has published a Directory of Cyber Security Service Providers (Note that customers can opt to contract with other providers that are not featured in the Directory) and published a new Directory of CSP Assessment Providers for customers' reference in seeking a company to perform the external assessment. (This complements the directory of Cyber Security Service Providers which remains).

Why is the back office not in scope, since this is also being attacked?
A: Even if strictly speaking the back office is out of scope for attestation purposes, SWIFT still recommends users to use the security controls as a baseline to secure the whole end-to-end transaction chain.

If we are PCI-DSS, ISO27002, NIST certified, do we still need to comply with SWIFT's Security Control Framework.?
A: Yes. Compliance with other security frameworks may certainly be beneficial towards applying the same controls to the components in-scope for the SWIFT Customer Security Controls Framework. However, compliance with another framework is alone not sufficient unless a compliance analysis is conducted. To help users in such analysis, a mapping between commonly recognised standards such as PCI-DSS, ISO27002 or NIST and SWIFT security controls is provided in the annexe E of the SWIFT Customers Security Controls Framework.

© 2021 SWIFT

Are test and development environments in scope of the security controls?
A: **Test systems** are outside the scope of the security framework. However:

- If the test environment is not fully segregated from the live environment, the user should make sure that the same security controls apply as for the live environment
- If the test environment is fully segregated from the live environment, the user should still implement, good security hygiene such as malware protection, system hardening, physical protection of the servers, monitoring that no unexpected configuration changes are made.

The analogy can be made with Back-Office applications. These are also outside the framework scope, but still we strongly recommend customers to implement security controls.

Development systems that are not directly connecting to SWIFT Network do not need to be considered for the inclusion into the secure zone and in the CSP.

What is meant by monitoring in the following context: 'If the user's test systems are not fully segregated from the production systems, then they need to be secured to the same level and the customer should monitor carefully this environment as well' ?
A: For example, the user should monitor that this test environment is not being re-configured to be used for live traffic (for example monitor that at no moment in time, a live LT is being logged in from that environment). It is also important to monitor who access the systems. For example, the user should monitor that this test environment is not being re-configured to be used for live traffic (for example monitor that at no moment in time, a live LT is being logged in from that environment). It is also important to monitor who access the systems. Reconciliation between payments and end-of-day statements will not be relevant here.

Why are GLI and AU-NPP users not subject to the CSP?
A: The CSP programme applies to SWIFT users only; These are defined as duly registered users of S.W.I.F.T. SCRL. In the case of GLI, customers contract with the Joint Venture (JV) and not SWIFT SCRL; SWIFT SCRL is merely a shareholder of the JV. In other words, GLI customers do not qualify as SWIFT users and, consequently, fall outside the scope of the CSP. For AU-NPP, It is somehow the same, customers do not have any contract with SWIFT but with NPP Australia Limited. AU-NPP customers are consequently not SWIFT users and fall outside the obligations of the CSP.

What is the impact of outsourcing the operations and hosting of some SWIFT components on the definition of my architecture type?
A: The fact that a customer outsources the operations and hosting of some SWIFT components they own to a third party (typical SaaS model), does not impact its architecture type. Since the customer remains responsible and owner of the SWIFT components under this model, the same rule for determining the architecture applies as if the customer was hosting/operating these components itself. The difference is that the user will need to request clarifications from the hosting company on the compliance to the relevant CSP controls.

I am using a Messaging Interface with no concept of owner BIC of the license (for example: BESS), what is the architecture types of the BICs configured on this Messaging Interface?
A: As a rule, in such case, SWIFT would recommend that the customer who is the owner of (or the one operating) the Communication Interface attest as A1 while the other BIC codes to attest as A3 or B.

© 2021 SWIFT

Can I use a non-compatible or interim-compatible Messaging or Communication Interface and still be compliant with the CSP control 1.1 'SWIFT Environment Protection' (v2019)?

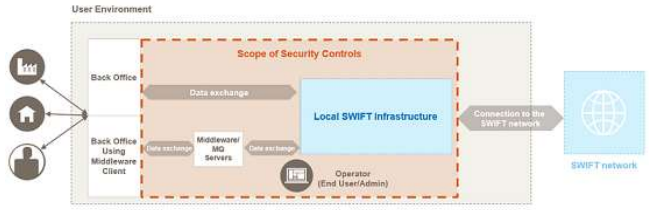
A: The CSP control 1.1 SWIFT Environment Protection (v2019) states in the Implementation Guideline section: 'All Messaging Interfaces (Alliance Access and equivalent) and Communication Interfaces (Alliance Gateway and equivalent) products within the secure zone are SWIFT-compatible. The list of compatible interfaces is maintained and published by SWIFT on swift.com.' However as this statement pertains to the Implementation Guideline section of the control, it means that any alternative implementation meeting the stated control objective i.e. 'Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment' and addressing the risks drivers could warrant a compliance with the control. In this specific case, the alternative solution would at the minimum rely on the implementation of controls that would compensate the missing customer confirmation for a 'interim compatible' Messaging or Communication Interface, or the non-compliance with the mandatory security controls listed in the security conformance statement associated with the non-compatible Messaging or Communication Interface used. The customer would need to attest for this control as *'I comply using an alternative implementation while meeting the same control objective'*.

As of 2019, the control 2.10A Application Hardening requires 'Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-compatible Messaging and Communication Interfaces and related applications.

Why, as of 2021, is the CSP/CSCF scope extended to middleware/MQ servers and what are the expectations going forward?

A: The scope of the CSCF v2021 is extended to cover, although still advisory, the middleware/MQ servers. The latter should be adequately configured to ensure safe data exchanges between SWIFT-related components in the secure zone and the Back Office (BO) first hop: the middleware/MQ servers indeed

1. validate the identification and authorisation of the data exchanges between those elements and
2. to be configured to enforce/ensure the security of data in transit.



Click here for the full size image

As per the graphic:

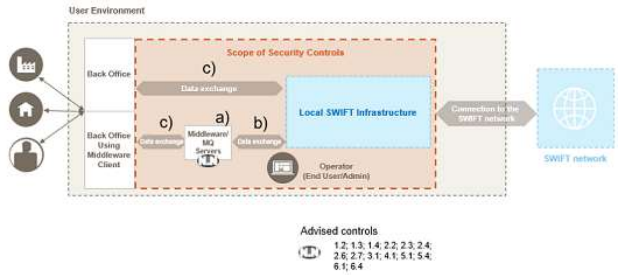
- The Back Office (using middleware/MQ clients) are out of scope.
- The SWIFT-related components are in the SWIFT Secure zone.
- The middleware/MQ server(s) are in a secure zone that has similar controls (advisory) – i.e. an operational environment with physical and logical controls (such as appropriate system admin, patching or vulnerability scanning surrounding processes). See next FAQ item for additional details on relevant Middleware controls.

© 2021 SWIFT

- Date transfer between SWIFT-related components and middleware/MQ servers they connect to are protected through secure protocols (as per the advisory control 2.4A).
- Data transfer between the middleware/MQ servers are protected through secure protocols (as per 2.4A).
- Ultimately, data transfer between middleware/MQ servers and the Back Office first hop (BO remaining out of scope) are end to end protected as per the control 2.4A.

Those controls will not be turned as mandatory for middleware servers in one go but are expected to be promoted gradually going forward. The scope of the security controls section of the CSCF should be taken into consideration starting from the, there defined, SWIFT-related components and user Back Office first hop to then identifying the middleware server(s) involved in data transfer between those elements.
Note: middleware/MQ servers independently used for non-SWIFT-related flows or behind the Back Office first hop are out of scope (even if SWIFT would strongly advise to protect them as if they were in scope).

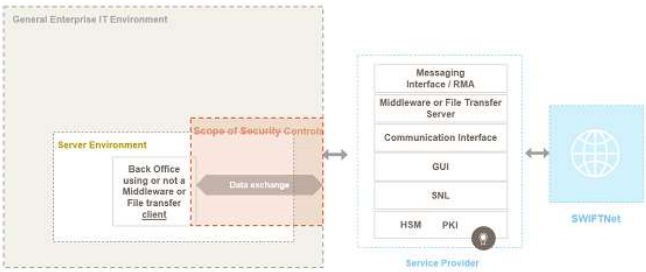
Which CSP controls will be applicable to middleware/MQ servers at the minimum and as of CSCF v2021?
A: As of the CSCF v2021, some CSP controls will be advisory* applicable to the middleware /MQ servers: they include 1.2; 1.3; 1.4; 2.2; 2.3; 2.4; 2.6; 2.7; 3.1; 4.1; 5.1; 5.4; 6.1; 6.4.



Click here for the full size image

* The mandatory controls have middleware server identified as advisory in their “in-scope components”

As a SWIFT user, I only use a client (Middleware or FTP) to connect to a server (Middleware or FTP) hosted at a service provider; what is my architecture type and what CSP controls are applicable to me?
A: Customers hosting only a client (Middleware or FTP) connecting to a server (Middleware or FTP) at a service provider or connecting their Back office directly to a service provider are considered as Architecture type B. This set up is illustrated in the picture below.



Click here for the full size image

© 2021 SWIFT

The following conditions apply:

- There is no parallel User to Application connections (i.e. PCs connecting to the service provider) on top of the app to app connection; and
- The service provider is a SB, L2BA or Group Hub and not an intermediary company hosting a Middleware or File transfer server that effectively belongs to the user.

The validation of those conditions is expected to be part of the community standard independent assessment mandated as of 2021.

SWIFT users with this app to app connectivity are subject to a limited number of CSP controls applicable to B; namely:

- 2.8A Critical Activity Outsourcing
- 2.11A RMA Business Controls
- 5.4 Physical and Logical Password Storage
- 7.1 Cyber Incident Response Planning

Is SWIFT planning to mandate controls 2.4A? If yes, what's the roadmap for changing the control from advisory to mandatory?
A: Control 2.4A will not be turned Mandatory in one go or in the short term; However, SWIFT is having the following roadmap:

- Starting with, when used, the security of middleware server and flows to the SWIFT-related components – (a & b) in the graphic above and
- Closing with the security of SWIFT-related flows towards the back office systems (first hop) – (c) in the graphic above.

Below guidelines are provided to users to gradually reach compliance:

- Establish an inventory of SWIFT data flows between SWIFT related components and the first back office hops (directly or via middleware)
- Establish a plan to implement/activate security mechanisms for the identified flows considering:
  - Implementing existing security mechanisms exposed by the interfaces, connectors, middleware server or the back office system;
  - Migrating opportunistically legacy and less standard flows to secure mechanisms or protocols;
  - and Mitigating, in the meantime, the risk of back office host spoofing or messages injection through systems or network connectivity means

What is meant by 'secure zone with similar controls as the SWIFT secure zone'?
A: A secure zone with similar controls as the SWIFT secure zone refers to an operational environment with strong physical and logical controls (including at the minimum and as appropriate system admin, patching or vulnerability scanning surrounding processes, presence of boundary protection and access controls and into the zone (see control 1.1).

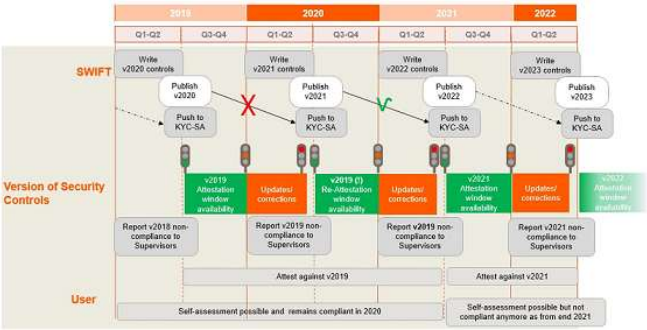
What are the CSP timelines for attesting, compliance, releases, consultation and reporting?

© 2021 SWIFT

A: Reporting to regulator: Reporting the customer's attestation status, and since 2019. Also the customers compliance status to their regulators happens twice per year.
Releases, Attestation & Compliance:

- A new version of the CSCF is released at the beginning of Q3 annually. From here on the preparations for assessment and compliance with the new/revised controls can start.
- Attesting against this version of the CSCF can start in Q3 till End of December of the same year, and is valid until the end of the year after the attestation has been published.
- Attesting should always be done against the controls of the CSCF that is current at that time.

Note: For any changes to the timelines related to Covid-19 please visit: Tip 5024006 - FAQ - Update to CSP timelines



Click here for the full size image

What are the actions needed when my attestation has expired?
A: Customers are requested, as per the CSP Policy, to always have a current valid attestation – to this end, SWIFT recommends users to re-attest before their attestation has expired (and turned amber). If their attestation has already expired, customers are requested to publish a revised attestation against the current version of the CSCF, and give the most up to date status of compliance for each relevant control. For controls that have yet to be assessed, an option is for customers to attest as 'I will comply by a given date' and enter a date for compliance. Note that attestations created after July 2019 will not expire till the end of next year 2020. However, If a customer has indicated 'I will comply by a given date,' it is considered as non-compliant and will need to be updated to " I comply" by the end of 2019 to avoid supervisory reporting.

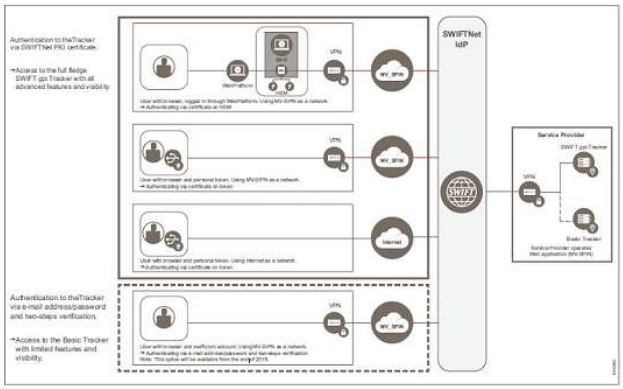
I am using a standalone GPI Connector, is this connector in scope and what is my Architecture Type?
A: SWIFT considers the standalone GPI connector as in scope and subject to the CSCF controls A3 (i.e. all CSP controls but the 6.3 Database Integrity). The rationale for considering this architecture as A3 is the fact that messaging capabilities (such as stop and recall) are implemented

What are the components in scope of the CSP when accessing the GPI Tracker Portal?
A: There are four ways to access to the GPI tracker:

- Option 1: for users having A1 architecture. in this case , all SWIFT components would be in scope: SAG/SNL, HSM, General Operator PC and Web platform. (Note that the VPN Box is specifically subject to the control 3.1 Physical security).

© 2021 SWIFT

- Options 2 & 3: for users having B architecture. In this case, the related controls would apply on the General operator PC. (Note that the VPN Box is specifically subject to the control 3.1 Physical security).
  Note: for the Options 1 to 3 – the CSP Logical access control (5.1) is consequently mandatory and mandates a segregation of duties (4 eyes)
- Option 4: for users connecting to GPI tracker via swift.com credentials . GPI actions from those general operator PCs are read only – i.e. No option to do a GPI Stop and Recall. In this setup, General Operator PCs are outside the scope of the CSP, however SWIFT strongly recommend to include them as per general cyber security hygiene.



[Click here for the full size image]

A control relevant to my architecture type is not applicable, how can I reflect that in my attestation?
A: Some controls can be flagged as Not Applicable (e.g. 6.1 Anti Malware Control). If this option is not available SWIFT recommends to

- Select "I comply using an alternative implementation while still meeting the same control objective"
- Specify in the "optional clarification" field: "Not applicable in our set-up".

Are the middleware server and data exchange layer in scope of the CSCF v2021?
A: In CSCF v2021, middleware servers are advisory in scope of a number of CSCF mandatory controls and can be considered out of scope by users. Data Exchange layer is an in-scope component of 3 advisory controls (including 2.4A) and one mandatory control (6.4 Logging and Monitoring). Hence, implementing middleware advisory controls is based on user's decision.

Is Alliance WareHouse (AWH) in scope of the CSP?
A: AWH is an application used to store long term messages; AWH is similar to a back-office application that does not allow messaging operations. Back office are hosted outside of the SWIFT secure zone. As this warehouse receives messages from the Messaging Interface, it is subject to the CSP control 2.5A External Transmission Data Protection whose objective is to 'Protect the confidentiality of SWIFT-related data transmitted or stored outside of the secure zone as part of operational processes.'

© 2021 SWIFT

In the CSCF v2021 what controls are applicable per architecture type?

A: See the table below:

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	■	■	■	■	■

Click here for the full size image

Back to Index

I am using a hosted database, which controls apply to the hosted database and the supporting server?

A: The controls applicable to the hosted database and the supporting server are summarized in the table below (v2021). As for the control 4.2 (Multiple factors authentication), the following rules apply:

- At the OS level, MFA is always applicable – subsequent connection by login from the OS into the database needs not be subject to MFA providing adequate database logical access (control 5.1) and application database integrity (control 6.3) controls are in place.
- Other connections to the database (i.e. **not** from the OS on the supporting server into the database) are subject to MFA. This MFA can be performed at the level of (in this order of preference) the (i) GUI to the database, (ii) on the jump server or (iii) on the dedicated operator PC.

© 2021 SWIFT

Mandatory and Advisory Security Controls	database	server
1 Restrict Internet Access and Protect Critical Systems from General IT Environment		
1.1 SWIFT Environment Protection	X	X
1.2 Operating System Privileged Account Control		X
1.3 Virtualisation Platform Protection		X
1.4 Restriction of Internet Access		X
2 Reduce Attack Surface and Vulnerabilities		
2.1 Internal Data Flow Security	X	
2.2 Security Updates	X	X
2.3 System Hardening		X
2.4A Back Office Data Flow Security		
2.5A External Transmission Data Protection	X	X
2.6 Operator Session Confidentiality and Integrity	X	X
2.7 Vulnerability Scanning	X	X
2.8A Critical Activity Outsourcing	X	X
2.9A Transaction Business Controls		
2.10 Application Hardening		
2.11A RMA Business Controls		
3 Physically Secure the Environment		
3.1 Physical Security		X
4 Prevent Compromise of Credentials		
4.1 Password Policy	X	X
4.2 Multi-factor Authentication	X	X
5 Manage Identities and Segregate Privileges		
5.1 Logical Access Control	X	X
5.2 Token Management	X	X
5.3A Personnel Vetting Process	X	X
5.4 Physical and Logical Password Storage	X	X
6 Detect Anomalous Activity to Systems or Transaction Records		
6.1 Malware Protection		X
6.2 Software Integrity		
6.3 Database Integrity	X	
6.4 Logging and Monitoring	X	X
6.5A Intrusion Detection		
7 Plan for Incident Response and Information Sharing		
7.1 Cyber Incident Response Planning	X	X
7.2 Security Training and Awareness	X	X
7.3A Penetration Testing	X	X
7.4A Scenario Risk Assessment	X	X

Back to Index

© 2021 SWIFT

1 Restrict Internet Access and Protect Critical Systems from General IT Environment

1.1 SWIFT Environment Protection

Our SWIFT servers are virtual. Must they be hosted on a dedicated ESX or can be hosted on an ESX containing other servers as well?
A: They can be hosted by other servers as long as all of them are compliant with the appropriate restrictions and controls in place. See section g.

Is it required that SWIFT components (within a segregated network) are in an independent and exclusive rack?
A: This is neither required nor necessary as per controls under principle 1, but do note that physical security controls need to be in place.

Is it mandatory to have separate Active Directory for the secure zone components? Or corporate Active Directory can be used instead?
A: To protect the corporate Active Directory, it is highly recommended that a separate Active Directory be implemented. This new instance need not be dedicated only to SWIFT components, but may be shared by other systems within the secure zone or with other secure zones. It remains the users' decision to implement an alternative option that meet the same control objective and addresses the same risk drivers, in which case this must be documented in the attestation.

Should archived SWIFT messages servers (Data Warehouse system, backup system, archive server, etc.) be in SWIFT secure zone?
A: As per the control 2.5A, archive servers storing sensitive data (like messages, credentials), have to be secured to prevent compromise of data backup or loss of sensitive data confidentiality.
That means either located in

1. SWIFT secure zone
2. another secure zone that has similar controls

ensuring appropriate encryption and adequate logical access to these archive servers. The data in transit also must be encrypted.

Please clarify 'remote administration'. Is it referring to a third party outside the organisation connecting to the secure zone? Or also a party within the organisation but not located in the same place/country?
A: Remote access to the secure zone from outside the local user network must be granted via the same secured channels as local operators.
This includes both

1. a remote administrator from an independent third party company contracted by the user to provide any portion of SWIFT-related services (for example, housekeeping in a Messaging or Communication Interface) to the customer and
2. user staff, agents or subcontractors working remotely.

© 2021 SWIFT

Can the firewalls that protect the SWIFT secure zone be shared (i.e. not dedicated to the SWIFT Secure Zone)?
A: The same physical firewall can be used only if it has the ability to have separate virtual instances (with separate OS loads in memory) and a separate virtual instance is used for the secure zone. A dedicated virtual firewall instance for the secure zone should be created. Separate policy configurations can not be used as a replacement to FW virtual instance.

Can I place the jump server to access the SWIFT Secure Zone outside of this zone?
A: As a rule, the security controls for the jump server must be as secure as the systems in the secure zone.By default , it should be inside SWIFT secure zone and abide to the zone controls. However, the alternative options are:

1. place the jump server in another secure zone providing that (i) similar controls are enforced (including the Identity and Access Management controls) and (ii) that the link between both secure zones is adequately protected (Confidentiality, Integrity and Authentication).
2. use a 'gateway server' outside the secure zone(s) (e.g. in a corporate environment) or at the boundary of the SWIFT secure zone to filter legitimate connectivity requests towards a jump server or SWIFT related components located in a secure zone. Identity and access management on the jump server and SWIFT related components still relies on authentication services offered within the SWIFT secure zone or in another existing secure zone that has similar CSP controls.

How to have a 'subset' of a mainframe to be defined as part of the SWIFT secure zone?
A: Some Mainframe terminology:

- LU: Logical Unit – a virtual instance on the mainframe that is capable of having isolated input/output
- SAF: System Authorization Facility - is the LDAP/Active Directory alternative for mainframes
- RACF: SAF solution provided by IBM, it has two alternatives as TopSecret and ACF2 by CA company. RACF can also be used to limit access on network level like iptables on Unix or windows firewall.
- OMVS: is the command that invokes Unix GUI on z/OS and zLinux is the Linux that runs on the z/OS. They have their own security mechanism that is also managed
- SYSOPER and SYSADMIN: are the default/built-in admin users in z/OS
- ICSF: is the built in HSM of the mainframe, it stores cryptographic keys and certificates.

Users can create a LU for the SWIFT related applications and apply the regular CSP security controls on the LU
As an alternative implementation, System Authorization Facility – SAF (e.g. RACF etc.) service (for z/OS including OMVS, zLinux etc.) will require implementing a comprehensive set of defence-in-dept controls to protect from and detect adversaries crossing the SWIFT related datasets and applications. Controls include:

- restricting access to the dataset to specific users,
- limiting highly privileged administrative accounts access (SYSOPER, SYSADMIN etc.) to SWIFT related data,
- implementing strong privileged access controls,
- implementing read-only access where feasible and
- enabling verbose logging

© 2021 SWIFT

- implementing centralized active monitoring and detective capabilities.

All other CSP controls should to be applied for the mainframe access including but not limited to Multi-factor Authentication, Internal, External Data Flow Security and Logging and Monitoring.

The following additional controls should also be in place:

- SAF functionality is advised to be used for network level restriction to access SWIFT related data only to specific application users. SWIFT related data should be encrypted in transit and stored encrypted.
- MQ channel encryption is not sufficient for meeting confidentiality and integrity criteria, the customer should use message level encryption methods supported by the vendor.
- Using a combination of TLS and related Integrated Cryptographic Service Facility (ICSF) functionality is advised to meet the control objectives of this control. More guidelines on cryptographic algorithms can be found in SWIFT Knowledge Center TIP 5021566.

Back to Index

1.2 Operating System Privileged Account Control

No article available for this control.

Back to Index

1.3 Virtualisation Platform Protection

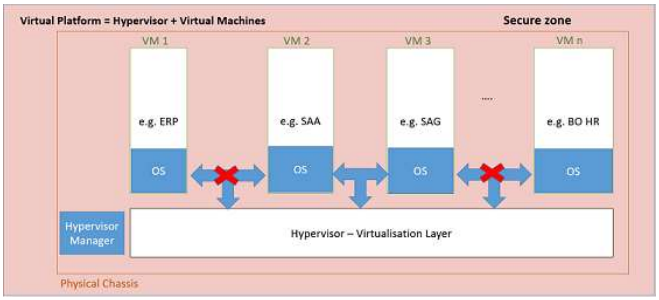
How do I attest if I don't have a virtualization platform?
A: As the option N/A is not available the workaround for attesting is to select "I comply as per alternative..." and say in the comment "not applicable".
In a future update of the KYC-SA application the N/A option will be made available for this control.

How is a typical virtualised environment look like in the context of CSP?
A: VM's isolation is ensured on the virtualisation platform to prevent **a)** lateral move out of a virtual machine to access or interact with other VM's or the underlying hypervisor or **b)** bypassing normal network controls that filter and/or inspect connections to the SWIFT environment.

- Filtering and expected inspection of the network flows reaching the SWIFT-related VMs are performed preferably using resources (such as FW, packet inspections or content filtering) external to the virtualisation platform or must be enforced at the hypervisor level.
- Provided that isolation is ensured on the virtualisation platform, the hosted VM's can keep their (security) classification and be individually secured accordingly (as such, they would not inherit the classification of the SWIFT related VM's and be subject to all SWIFT related controls).

this is graphically represented as:

© 2021 SWIFT



Click here for the full size image

When using containers, is it acceptable to share the underlying infrastructure OR is it necessary for SWIFT components to be completely isolated ?

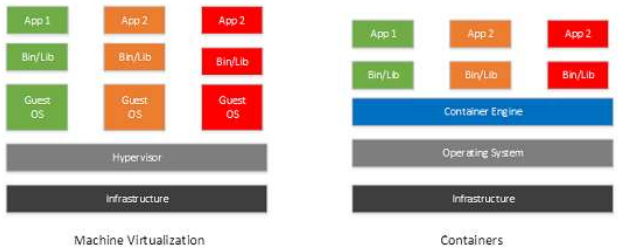
A: Containers are a software packaging method. While the word hints at separation, containerization does not automatically embed security. There may be very secure implementations however these are very complex and not often encountered (may further evolve in future).

Containers share the underlying OS, therefore running containers on the same host should be seen as similar to co-hosting the applications (Virtual machines do not share the Operating System and are therefore accepted, as long as there is network segregation.).

When Swift applications are in containers, all containers that share the same OS, even if they are not related to Swift, should be in scope of all applicable controls for the secure zone hosts and application of the Security Control Framework.

Example:*the admins for any non-Swift applications fall under same controls as the admins of Swift applications, as they may also get access to the Swift applications.*

However, SWIFT does not recommend using multiple shared layers between the containers (container engine, OS). The only exception is if a thorough risk assessment of potential lateral movement is performed between containers with different security classification hosted on the same infrastructure. SWIFT systems (secure zone) should be logically separated from non-SWIFT related ones (not share same OS) and network filtering should be in place. [Control 1.1 of the Customer Security Controls Framework] and SWIFT plans to extend the in scope components of CSCF control 1.3 to include containers.



Click here for the full size image

Legend

- Containers Engine is a container runtime for virtual environments that enables provisioning and management of applications packaged as Docker images into vSphere clusters.
- A hypervisor, also known as a virtual machine monitor, is a process that creates and runs virtual machines. A hypervisor allows one host computer to support multiple guest virtual machines by virtually sharing its resources, like memory and processing.

© 2021 SWIFT

- Virtualization enables running multiple operating systems on the hardware of a single physical server.
- Containers enables deployment of multiple applications using the same operating system on a single virtual machine or server.

Our SWIFT servers are virtual. Must they be hosted on a dedicated hypervisor or can be hosted on an hypervisor that is shared with other servers ?
A: Hypervisors can be shared with non-SWIFT servers , however control 1.3 "Virtualisation Platform Protection" must be followed to mitigate any risks on SWIFT servers. Implementation guidelines can be used to ensure the appropriate implementation of this control.

Back to Index

1.4 Restriction of Internet Access

How can I comply with the CSP control 1.4 Restriction of internet access when using General Purpose Operator PC (Fully managed or unmanaged device)?

A **fully managed device** is a company-owned device with features giving the company IT admins, control over the device settings and policy configuration. Conversely, **unmanaged devices** are individuals' own device used to access the company resources, network or applications hosted in the cloud or by a service provider. **Intermediary models** exist where managed (sand-boxed) application(s) (by a company) are deployed on the users' own device. All those models have to be properly analyzed for proper and secure usage.

In relation to a fully managed device, the Implementation guidance section of the control 1.4 suggests some potential options, specifically:

Internet access from general-purpose operator PCs (control 1.4, point 'b')

- Control internet access provided on the general purpose operator PCs used to
  - connect to an application at the service provider (user-to-application) to process financial
  - access a messaging or communication interface through a browser-based GUI (for example, Alliance Web Platform)

Through one of the following options:
1. Internet access through a remote desktop or virtual machine solution
2. Internet access from the general-purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
3. Internet access from the general-purpose operator PC through a Web Gateway (with content inspection, in combination with blocking/filtering controls) using maintained blacklisted URL destinations

Even if SWIFT strongly recommends to control internet access, another way to meet the control objective on those PCs accessing the local SWIFT infrastructure is to enforce usage of a jump server

© 2021 SWIFT

that has no internet access combined with multi-factor authentication, in line with control 4.2, implemented on the individual SWIFT related applications/systems or at the jump server

In case of **unmanaged** device such as when using (bring) your own device - BYOD, the following options should be considered:

- Based on a comprehensive risk assessment, the user should establish organizational policies and guidelines to enforce the safe use of unmanaged device requiring the implementation of controls to:
  - ensure proper authentication (e.g. PIN Code), activities authorization (with possible additional independent factors)
  - require appropriate and prompt user reaction, in case of device compromise, loss or theft, to block potential rogue access through such device
  - Comprise Antivirus, system updates
- Request IP filtering or jump server similar from the provider (I2ba, Service bureau or intermediary)

Back to Index

2 Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security

Is MQ channel encryption sufficient (IBM MQCE) for internal data flows within the secure zone?
A: As per control 2.4A, Confidentiality, integrity, and mutual or message level based authentication mechanisms are implemented to protect data flows between SWIFT infrastructure components and the back office first hop they connect to.
Encryption ensures confidentiality between internal data flows. Hence, additional mechanisms should be implemented to ensure integrity and authentication. Refer to control 2.4A for more details related to implementation guidelines.

Is LAU alone sufficient between the Messaging Interface and Communication Interface?
A: No, LAU only provides Authentication and Integrity while the connection requires Confidentiality, Integrity and Authenticity.
To ensure Confidentiality a layer of encryption needs to be added, for example: TLS or AES-GCM (AES-GCM is another solution referred in the CSCF that is embedding both (encryption and authentication).

Can we use SSL, TLS 1.0 or 1.1 between the components in the secure zone?
A: SSL as a technology is deprecated and must not be used. TLS is considered the successor (version of TLS to be used is >= 1.2). For more information see: Tip 5021566 - Guidance and Best Practices for Cryptography

Can all the compatible vendor products connecting to the SAG/SNL provide encryption and/or authentication and/or integrity, how is this being managed by SWIFT?
A: Along with Alliance Access 7.3 and later versions, any compatible vendor product must use confidentiality, integrity, and mutual authentication mechanisms (such as 2-way TLS, or LAU in

© 2021 SWIFT

combination with a confidentiality protection) to protect data flows with other systems in the secure zone.
This includes following data flows:

- GUI to Messaging Interface
- RMA application to Messaging Interface
- GUI to Communication Interface
- Messaging Interface to Communication Interface

More information related to the compatible vendor products can be found on swift.com: https://www.swift.com/about-us/partner-programme/swift-certified-interface-programme/document-centre

Back to Index

2.2 Security Updates

When there is an OS security update, does SWIFT have a proactive approach to test this update for their products before they broadcast the information to the community? Will the SWIFT product matrixes be updated accordingly?
A: SWIFT updates the product matrixes whenever a new version or update of a SWIFT product is released, not when a new service pack or other change(s) to the OS is applied and/or released by the vendor. Support and qualification of SWIFT products is performed as follows:

1. SWIFT publishes an 'OS levels and patches Baseline' document that specifies the OS version (including service packs etc.) that are used to qualify our software. This is the lowest OS version that SWIFT supports.
2. KB Tip 1212959 contains a statement regarding our support for OS versions that are higher than the baseline published by SWIFT. We will support any higher minor OS version by default. In the event that SWIFT discovers a problem with a service pack/security patch, these are blacklisted accordingly (see KB Tip 2224150). This is a reactive process, SWIFT does not proactively verify or check service packs or security patches on any OS.

Some vendors do not provide a CVSS scoring when they distribute patches, how does SWIFT propose we manage this?
A: SWIFT only provides a security risk (CVSS) score for SWIFT software. It is the responsibility of each user to apply updates for any other software in accordance with their own internal policies and risk management framework. To help users, SWIFT has provided recommendations based on the availability of a CVSS score.

Can general IT environment patching server be used to push updates to secure zone servers?
A: Yes, but CSCF controls must be applied , especially control 1.1 and 2.2 .Implementation guidelines include but not limited to:

- Login credentials should not be stored outside the secure zone.
- Strict firewall rules between patching server and SWIFT servers.

Back to Index

2.3 System Hardening

© 2021 SWIFT

Does SWIFT provide guidelines for hardening components in scope of control 2.3 "System Hardening" ?
A: Control 2.3 “System Hardening” implementation guidelines provide recommendations for hardening. These recommendations include the following:

- Vendor security configuration guidance. SWIFT provides guidelines for hardening hosts running release 7.4 of Alliance Access, Alliance Entry, Alliance Gateway, Alliance Web Platform Server-Embedded, SWIFTNet Link, or release 4.0 of Alliance Messaging Hub. Also SWIFT provide security guidance for hardening their products like Alliance Access.
- Industry-standard security configuration guidance (for example,6 CIS , DISA STIG, NIST),
- A local or regulator's standard security configuration or controls set of the same rigour as the vendor or industry guidance.

Can you provide an example of “vendor security configuration guidance” found under section 2.3?
A: As an example IBM provide “Vendor Security Configuration guidance" with their AIX operating system.

Back to Index

2.4A Back Office Data Flow Security

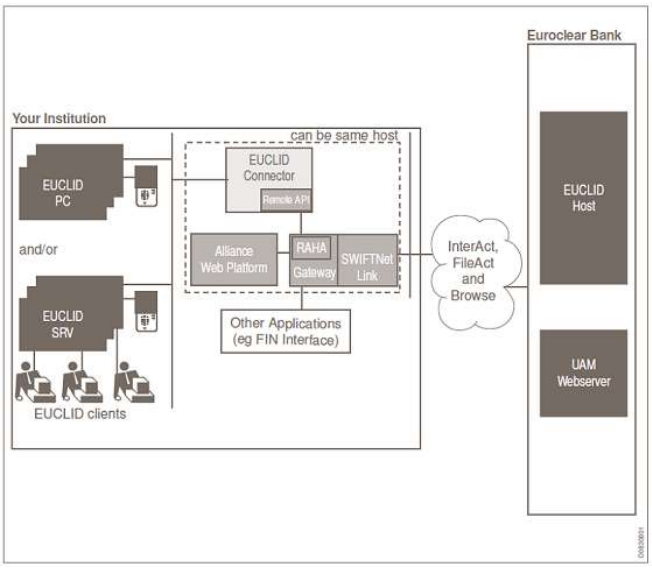
Our back office application supports TLS but does not support LAU. What can we do?
A: LAU is a technology developed by SWIFT for the authentication and integrity of the exchanged data.
Besides the technology developed by SWIFT there are others that can be used to meet the control objectives, where some are already mentioned in the CSCF (XML DSIG, AES GCM Authenticated Encryption, 2-way TLS).
An example where 2-way TLS can be used as an alternative for LAU: Certificate based authentication between the WebSphere MQ server and the MQ client on the Alliance Access side.

More details on the supported versions of TLS can be found in Tip 5021566 - Guidance and Best Practices for Cryptography

How can I implement the control 2.4A in the specific use of Euclid Connector (ECC) / Alliance Gateway connectivity?
A: The security of the Euclid Connector / Alliance Gateway relies on the combined implementation of

- TLS on the segment between the EUCLID Server/PC to Euclid Connector with
- the use of EuroClear certificates that secure connection from Euclid PC/Server to Euclid Host which includes the segment Euclid Connector – SAG (as illustrated in the diagram below). SWIFT recommends using the latest version of the ECC to benefit from the latest security features.

© 2021 SWIFT



Click here for the full size image

Back to Index

2.5A External Transmission Data Protection

What other types of data (other than the ones mentioned in the control) are considered by SWIFT to be sensitive?
A: As a general principle, data sensitivity is categorised based on the customer's own internal security policies and risk profile. Related local laws and regulations that apply to the organisation which must be taken into account. Sensitive SWIFT data would include such as back-ups, business transaction details and credentials.

Back to Index

2.6 Operator Session Confidentiality and Integrity

Is it possible to use self-signed certificates for HTTPs user sessions or it's recommend the use of certificates provided by an internal or external Certificate Authority (CA)?
A: Self-signed certificates are certificates generated from an untrusted certificate authority. By using self-signed certificates to secure HTTPs sessions, these sessions can be subject to MITM (man in the middle) attacks. These attacks are not easily identified because the users get used to the warning message issued by the browser due to the use of self-signed certificates.
SWIFT recommends using certificates issued by trusted internal or external CAs (certificate authorities).It's well known that some organizations may have technical or budget limitations that prevents from obtaining trusted certificates. Hence, it is the organization responsibility to conduct a risk assessment to identify associated risks and apply the suitable controls that mitigate these risks. The controls can include the following:

- Storing the private keys on HSM.
- Applying 4 eyes for CA maintenance.
- Strict logical and physical controls on server issuing the certificates

© 2021 SWIFT

Can I mitigate this control against a PC timeout (i.e. screen lock)?
A: This control addresses all sessions into the secure zone: browser, applications and operating system shells. These sessions may or may not involve a PC. Screensavers are an additional mitigation but not sufficient to meet this control because a process on the PC could hijack an active session or if the screen saver was bypassed (e.g. with key logger) then an attacker could instantly have access to all active sessions.

When a user is connected (and idle) to a Browse or GUI application, should the session lock or logout?
A: You can choose, both the lock-out or log-out mechanism can satisfy the control requirements.
An inactivity lock-out feature that limits the session to the minimal timeframe necessary to perform business-as-usual duties would be considered as sufficient to meet the objective of the control and address the risk drivers.

Back to Index

2.7 Vulnerability Scanning

Can SWIFT assist in performing vulnerability assessments or penetration tests?
A: No, SWIFT does not provide or advise on these services. Users that do not have this expertise or would like to increase their capabilities can engage the support of a third-party Cyber Security Service Provider. A directory of such providers is available on the CSP community engagement page of swift.com.

We have a UNIX/LINUX environment, is vulnerability scanning also required?
A: This control is system agnostic and applies to all systems within the secure zone and to any system accessing the secure zone.
Vulnerability scans can be conducted against any system, a customised test can be done per system based on its services and platform.

Can we use an "external to secure-zone" vulnerability scanning solution, or should there be a dedicated solution that is fully contained within the security zone?
A: SWIFT recommends a dedicated scanning solution fully contained within the secure zone. It remains a users' prerogative to implement an alternative option that meets the same control objective and addresses the same risk drivers.

Under the implementation of the control you say "Vulnerability scanning is performed at least annually as well as after any significant change…" Please clarify "significant change"?
A: It is up to each user to determine for itself what "significant change" means based on its threat exposure, risk tolerance and security policies and other requirements. SWIFT does not provide a universal definition bearing in mind however that significant changes that would require a vulnerability scan include (without limitation) a new server or a change of OS in the secure zone. If a user needs assistance in area, it can engage the support of a third-party Cyber Security Service Provider.

Is vulnerability scanning mandatory or not for general operator PC ?

© 2021 SWIFT

A: No it is not mandatory, however it's considered an optional enhancement.

My architecture is categorized as Architecture type B and read, in v2021, that the control 2.7 Vulnerability Scanning is advisory – how can I attest this year against this control in KYC-SA?
A: At this moment, the control 2.7 cannot be flagged as 'Not Applicable' for Architecture type B; consequently SWIFT Recommends users to attest as:

- Select *"I comply using an alternative implementation while still meeting the same control objective"*
- Specify in the "optional clarification" field: *"Not applicable in our set-up".*

Back to Index

2.8A Critical Activity Outsourcing

What type of details should this Service level agreement (SLA) include, can SWIFT elaborate?
A: In case of outsourcing, each user is responsible for determining an appropriate contractual framework including (without limitation) well-defined and relevant service levels, monitoring and reporting arrangements and remedies. Users must also consider any specific outsourcing requirements that may apply to them under applicable laws and regulations.

Under this control what are considered outsourced activities - is it activity done by a vendor or partner? What if the activity is done on our premises by a vendor or partner?
A: Any activity that is not directly performed by or on behalf of the attesting user is considered as outsourcing. The objective of the control is to ensure that outsourced activities are equally secure or even more secure than if they had been conducted in-house.

Back to Index

2.9A Transaction Business Controls

What does SWIFT consider being normal business hours?
A: Business hours are organizational and business unit specific. Multiple start and finish times (business hours) may need to be supported.

What options are available on the SAA to meet this control, specifically with regards to gaps in the sequence number?
A: The implementation of this feature is further detailed in the SAA Security Guidance documentation.

Back to Index

2.10 Application Hardening

No article available for this control

Back to Index

2.11A RMA Business Controls

© 2021 SWIFT

No article available for this control

Back to Index

3 Physically Secure the Environment

3.1 Physical Security

Would a logical segregation compensate whereby only members of the Active Directory (AD) group are entitled to use the PC?
A: No, the risk to address with this control is to ensure that only persons authorized to work on the SWIFT-related workstation have physical access to the PC (e.g. business end user, Administrators, Supervisor ...). Physical protections should be implemented in addition to any logical protections.

Should environmental threats (fire, flooding, earthquake, heat, etc.) also be considered for this control?
A: Environment threats (fire flooding, earthquake, heat, etc.) are not part of the cyber security threat landscape and as such are not included in the scope of the SWIFT Customer Security Controls Framework, but should be covered by other business continuity procedures.

Is it required that SWIFT components are physically segregated from other general enterprise IT environment ?
A: SWIFT components are not mandatory required to be physically segregated. However , control 3.1 "Physical Security" must be applied for all components in scope.

Back to Index

4 Prevent Compromise of Credentials

4.1 Password Policy

Do the <password> requirements take into account other safeguards such as 4 or 6-eye release of transactions?
A: No, the 4 or 6-eye processes do not combat weak passwords.
The segregation of duties (5.1 - Logical Access Control) and password management (4.1 - Password Policy) need to be implemented in addition to each other.

Should both the Passwords and PIN comply with the Password policy (4.1) control?
A: Yes, both the PIN and passwords must comply with the password policy.
A PIN is not considered a password, however PIN's are covered in this control. The rules for PIN codes should be incorporated in the Password Policy.
More information and guidance on passwords and PIN's can be found in Tip 5021567 - Guidance and Best Practices for Passwords and PIN Policy Principles.

Back to Index

4.2 Multi-factor Authentication

© 2021 SWIFT

Is 2FA required for Browse or WebAccess services?
A: Yes, in most cases, (see next question/answer describing cases when this is not required). With Browse, the authentication can be provided by the Server application which is often not provided by SWIFT. For WebAccess, the authentication is always based on a SWIFT PKI certificate, which can be stored on a personal token, or in HSM and used through SAG/SWP. 2FA capability for SWIFTNet users defined on the SAG for using the WebAccess GUI might be considered for implementation in future releases. Already today, Customers could implement 2FA for their WebAccess GUI users over Virtual SWIFTNet Users in combination with RADIUS, LDAP solutions.

Is the MFA security control also mandatory to access Browse services that are purely used for monitoring/inquiry or consultation purposes, such as balance query, queue management?
A: As conceptually, there is no integrity risk for anyone using Browse services only designed for monitoring/inquiry, customers could attest as compliant in an alternate way.

Do users of a service bureau have to use the Multi-Factor Authentication (MFA) solution offered by their service provider on their Messaging Interface to comply with the control 4.2?
A: Service bureau must offer to their customers an MFA solution to be compliant with the SIP Program. It remains however the service bureau's customers' prerogative to opt out of the offered MFA solution and to implement an alternative implementation. However, this alternative implementation must meet the following criteria:

- Allows meeting the control objective of the control 4.2, namely: 'Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.'
- Mitigates the risk drivers listed in the control; namely:
  - Credential replay
  - Password cracking, guessing, or other computational compromise
  - Password theft

The SWIFT's implementation guidelines natively list three options for the end users access to the secure zone – in descending order of security robustness:

© 2021 SWIFT

#	Option	Use case for service bureau customers
1	On the individual SWIFT applications (on the browser-based GUI, on the Messaging Interface, or on the Communication Interface)	acceptable
2	At the secure zone boundary (jump server)	The secure zone in this case is the one located at the service bureau. This option is available to customers of a service bureau. When this option 2 is made available to SB's customers for using their own IdP (identity Provider), it has to be properly configured, designed together/in cooperation with the Service Bureau (and that will probably require costs, resources, time)
3	At the dedicated operator PC log-in. (that is An operator PC located in the secure zone and dedicated to interact with components) –	This option is not available for customers of a service bureau

Note that the MFA solutions implemented under option #2 or as an alternative implementation will be checked by SWIFT in the context of the audit supporting the SIP Certification programme.

Do users of a L2BA provider have to use the Multi-Factor Authentication (MFA) solution offered by their service provider on their Messaging Interface to comply with the control 4.2?
A: L2BA provider must offer to their customers an MFA solution to be compliant with the L2BA Program. It remains however the L2BA provider customers' prerogative to opt out of the offered MFA solution and to implement an alternative implementation. However, this alternative implementation must meet the following criteria:

- Allows to meet the control objective of the control 4.2, namely: 'Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.'
- Mitigates the risk drivers listed in the control; namely:
  - Credential replay
  - Password cracking, guessing, or other computational compromise
  - Password theft

© 2021 SWIFT

The SWIFT's implementation guidelines natively list three options for the end users access to the secure zone – in descending order of security robustness:

#	Option	Use case for L2BA customers
1	On the individual L2BA applications (on the browser-based GUI)	acceptable
2	At the secure zone boundary (jump server)	The secure zone in this case is the one located at the L2BA provider. This option is rarely available to customers of L2BA provider and would allow L2BA customers to access the application or any other component of the L2BA provider by passing the GUI. When this option 2 is made available to L2BA provider 's customers for using their own identity Provider (IdP), it has to be properly configured, designed together/in cooperation with the L2BA provider (and that probably requires costs, resources, time)
3	At the dedicated operator PC log-in. That is an operator PC located in the secure zone at the L2BA provider and dedicated to interact with components.	This option is not available for customers of a L2BA provider

Note that the MFA solutions implemented under option #2 or as an alternative implementation will be checked by SWIFT in the context of the audit supporting the L2BA Certification programme.

When a PIN Code is requested for a token (for example a RSA token), is a Password and user ID login still required to comply with the Multi-factor Authentication control?
A: In the context of Multi-factor Authentication, a Token will be considered as a Possession factor. A Complex PIN code (a succession of numbers by definition aligned with the complexity documented in the SWIFT PIN Policy) would be a valid knowledge factor. If these conditions are met, PIN and a (RSA) token would be a valid Multi-factor Authentication solution. If the PIN code is not strong (e.g. 4 characters), it would need to be complemented by a strong password.

© 2021 SWIFT

Back to Index

5 Manage Identities and Segregate Privileges

5.1 Logical Access Control

Does segregation of duties also apply to SWIFTNet browse users accessing a browse provider?
A: Yes, the scope covers all operator accounts, both local to the secure zone, but also those used to access services you connect to from the secure zone. That includes (but not limits to) Online Operations Management (O2M), but also third-party services.

I am using shared certificates, is this OK?
A: Using a shared/generic certificate may not be breach of the accountability concept (and thus does not contradict MFA or Logical access control) – providing the customer's internal controls system warrants an identification of the entity."
In other words, the usage of these generic accounts is not a breach of the CSP accountability concept, providing the banks have an internal system to clearly identify the end user behind the generic account.

Back to Index

5.2 Token Management

What are the requirements for managing HSM using remote PED keys in the context of CSP?
The Remote PED mode is a feature that allows users to manage an HSM box from a distant location using a Remote PIN Entry Device (PED) and PED Keys. The HSM box can communicate with the Remote PED over a LAN or WAN. The Security Officer (SO), User, or Domain keys can be used to operate the HSM box using the Remote PED mode from their administrative office and do not require physical access to the datacentre where the HSM box is located.
If the Remote PED workstation is outside the secure zone, a PC dedicated to this functionality should be used. Local authentication is preferred on that workstation but limited access, patching and system hardening should be in place. Furthermore, the following points should be taken into consideration:

- Ensure compliance with the CSP control 5.2 Token Management (CSCF Page 56) regarding management of the PED keys and the remote PED activities, namely: The flows to the HSM must be secured as per the Alliance Security Guidance asking to limit software deployed on the remote PC. Such PC should be dedicated to remote PED activities and not a standard General Purpose Operator PC.
- As the remote PED activities cannot be performed over a jump server, the customer needs to open some specific ports on the firewall protecting the secure zone so that this remote PED PC, can access the Server hosting the SNL:
  - HSM Proxy on the SNL host to be able to connect to port 48322 on Remote PED server host
  - HSM appliance able to connect to port 48321 on SNL host (on which we run HSM Proxy)
- Once the remote PED activities have been performed, the ports on the firewall need to be closed – this should not represent a burden as this is no daily types of activities but rather exceptional activities (at the end that is customer's prerogative to conduct a risk assessment as to the risk of leaving these ports permanently open or not)

© 2021 SWIFT

Back to Index

5.3A Personnel Vetting Process

No article available for this control

Back to Index

5.4 Physical and Logical Password Storage

No article available for this control

Back to Index

6 Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection

Should any application files or folders be exempt from anti-malware scanning?
A: SWIFT does not recommend exempting any files or folders from anti-malware solution by default. SWIFT recommends that anti-malware software is tested and configured for compatibility with the specifics of your operational environment. For more information see Tip 5020533.

Back to Index

6.2 Software Integrity

What integrity checks are available in SWIFT products and vendor supplied products?
A: For SWIFT products, please consult the relevant technical and security guidance documents. For 3rd party vendor supplied products, contact the vendor concerned directly.

- **SWIFT products Security Guidance documents:**
  - Tip 5020786 - Security Guidance
- **SWIFT products technical documents:**
  - Alliance Entry 7.3
  - Alliance Access 7.3
  - Alliance Messaging Hub 4.0
    - database integrity (chapter 3)
    - file integrity (chapter 2.7)
  - Alliance Web Platform 7.3
    - database integrity
    - file integrity

Back to Index

6.3 Database Integrity

© 2021 SWIFT

What integrity checks are available in SWIFT products and vendor supplied products?
A: See 6.2 Software Integrity: *"What integrity checks are available in SWIFT products and vendor supplied products?"*

We own only the SAG, what is my architecture type and is the control 6.3 Database Integrity applicable?
A: The fact that you own a Communication Interface renders you A1, however in this case, the control 6.3 Database Integrity is not applicable, and must be marked as ' I comply using alternative implementation meeting the same control objective' and indicate *'No Database to which this control applies in our environment'* in the optional comment.

Back to Index

6.4 Logging and Monitoring

Is it required to have audit logging (CSP Control 6.4) on SWIFT gpi tracker and if so, how can it be implemented?
A:

- In case of usage of the basic GPI tracker (only for viewing purposes), the tracker is considered as out of scope of the CSCF (Click here for Information about the 'standalone GPI connector')
- In case of usage of the Stop/recall functions in the GPI tracker, the GPI infrastructure falls in the scope of the CSCF (including the GUI) and specifically the CSP control 6. 4 – Logging and Monitoring applies. At this moment, there is no audit log facility on the gpi GUI for administrators to be able to view which user(s) took which action(s). This is currently in the development backlog with an estimated deployment in 2021. Dependent on the user setup , the logs available on SAG or the Webplatform can be used to retrieve some useful logs that compensate for the current lack of GPI GUI audit.

Back to Index

6.5A Intrusion Detection

No article available for this control

Back to Index

7 Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning

No article available for this control

Back to Index

7.2 Security Training and Awareness

© 2021 SWIFT

No article available for this control

Back to Index

7.3A Penetration Testing

Must all the installed software and all hardware components in scope of the secure zone be subject to individual penetration tests, or is penetration testing to be done on the overall secure zone?
A: The defined scope is not only on an individual level of the components, but to cover the sum of the components.
Penetration tests are based on simulated attacks that use similar technologies to those deployed in real attacks.
Conducting these simulations is an effective tool for identifying weaknesses in the environment which may require correction, improvement, or additional controls.

Must penetration testing be performed in the production environment?
A: For network component and hosts, penetration testing (for example, rule based and configuration review) is performed in the service production environment. Sufficient safeguards must be in place to minimise any operational impact from conducting the penetration test

Can you clarify what is meant with penetration testing after “significant changes”?
A: It is for each user to determine what "significant change" means based on their threat exposure, risk tolerance and security policies and other requirements. While these requirements will differ from user to user, typical examples of significant changes include the installation of new hardware or migration to a new OS. If a client needs assistance in this area, it can engage the support of a third-party Cyber Security Service Provider. SWIFT will shortly (This FAQ will be updated when the date has been confirmed) make available a list of such providers on swift.com.

Can an independent party perform the penetration testing for the user, whilst the vulnerability scanning is performed by internal staff?
A: Users can use an independent third party to conduct their penetration testing. When contracting with the firm of their choice, the user must make sure that all appropriate arrangements and controls are in place to ensure (continued) compliance with all controls and other requirements applicable to the user.

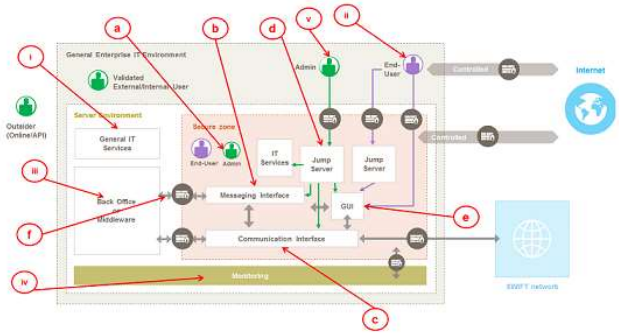
What is the scope of penetration test?
A: The focus of the CSP control Penetration test (7.3) as reportable in the KYC-SA application is the secure zone hosting the SWIFT components. All components in the secure zone and "in-scope components" in the CSP control 7.3 must be considered. The scope of a penetration test depends on how the user defines the secure zone. Defined scenarios take into account the attackers' perspective: i.e. that could be someone such as:

1. an unauthorised external user
2. a valid (authenticated) internal or external user or
3. a malicious insider (employee or other)

Examples of (non-exhaustive) attack scenarios are depicted in the graphic below and are mapped to attack vectors such as:

© 2021 SWIFT

- Privileges escalation on SWIFT components **(a)**,
- Unauthorised access to the Messaging Interface (e.g. SAA) **(b)**, Communication Interfaces **(c)** (SAG), Jump Server **(d)**, GUI **(e)**, HSM or VPN hosts or
- Account manipulation to elevate users' rights due to wrong settings on SWIFT Components or on data exchange layer components **(f)** such as routers, switches and firewalls or un-properly/un-securely configured protocols.



Click here for the full size image

SWIFT suggests using a standard framework to analyse possible attack vectors to the local infrastructure and integrating previous attack information shared on ISAC portal as a baseline when defining the scope of the penetration tests. It is the role of the penetration testers to identify the most critical or "sensible" elements considering the user' specific environment/architecture, if necessary expanding the scope of the tests to simulate a real attack.

Note: SAA, SAG and HSM products are already penetration tested at SWIFT; obviously, the underlying systems specific to the user environment are not. Users wishing to test on or through SWIFT-related services and products must comply with the SWIFT Customer Testing Policy.

Finally, SWIFT recommend users, as part of their penetration testing programme, to extend penetration tests beyond the SWIFT Secure zone to take into accounts IT assets not located in the secure zone as potential targets or entry points for attacks:

- Users' entry points **(i)** like:
  - Exploitation of vulnerable secure protocols and cipher suites
  - Escalation of Privileges at host/system level
  - Bypass of accounts controls
- Authentication mechanism **(ii)** and **(v)** attacks like:
  - Bypass of accounts controls
  - Escalation of Privileges at system/domain level
  - Forced Authentication exploiting application flows or interactive flows

Furthermore, even though not in the scope, the testing against the following attack scenarios is also recommended:

- Operational/monitoring infrastructure (as used by internal users/admin) **(iv)** and **(v)**
  - Escalation of Privileges for unauthorised access to the secure zone or to back office middleware/ applications
  - Abuse of Remote Services for unauthorised access to the secure zone or to back office middleware/ applications

© 2021 SWIFT

- Back office middleware/applications **(iii)**
  - Unauthorised message injection (File injection bypassing business controls)
  - Escalation of Privileges on host/system level for message modification

The Messages creation flows should also be covered end-to-end by the penetration testing programme, including (if applicable) the access from outsiders using online services or APIs and validated external/internal users.

Can I keep my secure zone connected to SWIFT whilst doing the penetration tests?
A: It is advised as per the SWIFT Customer Testing Policy, to disconnect the environment from SWIFT during penetration tests – the reason is that testing the system when connected could generate an integrity alert at SWIFT. As an alternative, users can perform the penetration tests on a true clone of their live environment. Note that it is also recommended to perform a vulnerability scan before any penetration test, as it already can hint some shortcomings on the live environment - a vulnerability scan is also not so intrusive.

Do I need to rebuild my environment after a vulnerability scan?
No, the systems to not have to be rebuild as Vulnerability scanning is considered as passive identification.
If further vulnerability tests are performed (beyond passive identification) it is considered a penetration test and the system(s) have to be rebuild as per the Customer Testing Policy.

Back to Index

7.4A Scenario Risk Assessment

No article available for this control

Back to Index

© 2021 SWIFT

How can I change my name and address details in KYC-SA?
A: To change the name and/or address (registered /operating address) of your institution, please submit the "Change your Legal or Publication information" e-form.
You will receive confirmation once the update is processed, and the change will automatically be reflected in KYC-SA shortly after (note however that this may take a few days).

What is the best practice for accepting/rejecting KYC-SA application access requests?
A: SWIFT strongly recommends its customers to consult their counterparties' attestation data and incorporate it into their risk management and business decision-making processes – alongside other risk considerations such as KYC, sanctions and AML. As customers request access to counterparties' data, so will the latter be requesting to access customers' attestation data. We recommend that you do not delay the processing of these requests. As best practice, you accept or reject access requests as quickly as possible and within a maximum of six business days.

To help you, we have created a video that explains how to grant access to other institutions to view your data in the KYC-SA application, and how to request access to view theirs. The video is available in the knowledgebase Tip 5021828

What level of information needs to be uploaded in the KYC-SA application (especially relevant if an institution does not adhere to the implementation guidelines)?
A: You will need to attest compliance with a control. If you don't follow the suggested guidelines, you can opt for an alternative implementation meeting the same control objective and addressing the same risk drivers. If you select this option, you may optionally provide information on this alternative.

Is a point in time or period of time requested for the attestation validity?
A: As per Policy, each user must attest once per year second half of the year. In case of changes, there might also be a need to update the attestation before the next annual attestation to reflect such changes. More information about the attestation timeline is provided in the Customer Security Attestation Policy

What is the legal ground for SWIFT reserving the right to report failures to comply with the mandatory attestation process to supervisors of supervised users (or to messaging counterparties for other users)?
A: Article 14.2.4 of the SWIFT General Terms and Conditions provides that SWIFT may report facts and circumstances relating to the security of the customer's use of SWIFT services and products such as the failure by customers to use a mandatory release or update of the software or, failures to comply with the customer security attestation process.

Why have the same controls for small clients as for large/complex MIs?
A: While a small subset of users - typically large or complex institutions - might consider alternative implementation routes for one or more controls, each and every user must attest compliance with all mandatory controls irrespective of the implementation solution ultimately deployed.

Do the controls apply by BIC, by entity, Or by group?

© 2021 SWIFT

A: Each user must attest for each BIC used in production. By default, groups will be configured so that the user at the top of the traffic aggregation hierarchy can manage the attestation process centrally for all BICs of all users in the group. Optionally, users can request a split of the originally provisioned group via a Support case.

What is the impact of not being compliant in the business relationship between users?
A: It remains each user's prerogative and responsibility to determine if and how the security posture as attested by a counterparty impacts their business relationship. Users are recommended to include the Security Attestation process into their regular Business Risk Management.

How do you protect data in The KYC Registry Security Attestation Application?
A: The KYC-SA application includes technical, physical, and organisational security controls to protect customer data against unauthorised access. SWIFT takes the protection of customer data very seriously and regularly carries out intrusion testing exercises to ensure the effectiveness of its controls.

Is the email from kycsa-no-reply@swift.com legitimate?
A: Even though the email is not signed, SWIFT confirms that kycsa-no-reply@swift.com is a legitimate SWIFT email address and can be trusted. It is used by the KYC-SA application to send the welcome emails and the notifications to inform the users about role changes, new actions, or information events.

When will I receive my welcome email for the KYC-SA application?
A: New customers get the welcome email as soon as their swift.com administrators have been assigned. Emails are sent by the KYC-SA application to the swift.com administrators of the parent destination in the traffic hierarchy.
A template of the welcome email can be found in Tip 5021947.

How can I find out who my swift.com administrator is?
A: Go to swift.com, log in to mySWIFT, go to *'my tools'* **>** *'my profile and account'* **>** *'search users'*, and follow the instructions in the Identity Management Online Help.

Why do I receive email notifications for missing roles?
A: As a KYC-SA administrator, you receive notifications by email informing you that your group is missing essential roles. The mails have as subject "Your update of tasks and information events" and are sent from <kycsa-no-reply@swift.com>. You will receive these notifications until you have assigned a Submitter, Approver, and Granter for your group of entities.
If you receive notifications while you have assigned the required roles, it's because the events in your KYC-SA inbox have not been dismissed (Inbox **>** For information **>** click dismiss in the status column). The email lists the 5 most recent events which haven't been dismissed;

You can select how often you want to receive these notifications via My Preferences **>** Information events. The default selection is set to once a week but you can update the frequency to daily, monthly or never. For more details, please refer to the user guide.

I have the granter/submitter role but am not able to grant or request access
A: You probably have different swift.com profiles and are logging in with the wrong one.
If you are registered on swift.com for multiple BICs, you have a specific user profile per BIC. Your KYC-accesses can be different for each BIC.

© 2021 SWIFT

When you login to swift.com, you must choose (in the 'list of profiles'- dropdown on the login screen) the BIC for which you want to submit data or grant access.
By default, the BIC that you used during your last connection is selected.

How long will SWIFT need before my attestation is published ?
A: The duration of SWIFT's qualification depends on changes performed by users in the architecture type section of their attestation. Furthermore it depends on the magnitude and responsiveness of the subsequent exchanges between the user and SWIFT. On a best effort basis, if no changes were made in the architecture type, connectivity and interface data, we estimate a publication within 5 business days. In case a change was made to previously mentioned data, we estimate the publication or rejection date, on average, to be performed within 12 business days.

What are SWIFT's expectations regarding the roles and responsibilities of an institution's CISO in the context of the CSP in general and the attestation process in particular?
A: SWIFT believes that the CISO of an institution is the stakeholder in the context of the CSP Programme; the CISO is responsible

1. for the assessment of the compliance of the institution's local SWIFT environment against the SWIFT mandatory security controls (and ideally the advisory controls),
2. for the definition and monitoring of the derived action plan to close the gaps identified during the compliance assessment phase and
3. SWIFT could possibly engage with the CISO in case of security incidents or just for relevant information sharing. In the context of the attestation process specifically, SWIFT requires the CISO to be the approver of the attestation, subsequently taking the accountability for the accuracy of the data submitted in their attestation.

How will SWIFT contact the CISO, SOC, or Payment Operations Contact of an institution?
A: SWIFT could possibly engage with the CISO, SOC, or Payment Operations contact in case of security incidents or just for relevant information sharing in the context of cyber security. SWIFT will choose the most appropriate channel to contact the CISO or SOC based on the level of emergency required (mail or phone). If further authentication is requested, SWIFT can reach out to the contact via either of the following channels (based on customer preference):

- The SWIFT Case Manager.
  Note that a case is visible to all users within your institution that have a valid swift.com account with the necessary permissions to access to the swift.com Case Manager. It is recommended to give your CISO and SOC contacts access to the Case Manager in advance. Not only will this allow for the authentication of the SWIFT contact, but it will also allow them to track and follow up on the SWIFT investigations.
  (PS: also the phone channel to reach Customer Support requires a valid registration number)
- E-mail originating from the swift.com domain.
  SWIFT e-mail sent from the swift.com domain implements SPF and DKIM. This provides reasonable assurance that the e-mail originates from SWIFT if these are checked by the receiver. It is up to your institution's discretion to verify that the e-mail originates from SWIFT.
- SWIFT Post e-mail.
  Upon request from customers only, and as a last resort, we will send a SWIFT post e-mail – attaching the PDF minutes of our earlier call with the SOC/CISO

© 2021 SWIFT

How to add/modify your CISO registration?
A: This information (name, contact details) must be self-maintained in the 'Contact details' section of the KYC-SA application.
It is possible to register several persons (e.g. CISO, Deputy CISO,...) via 'Add new'.

I don't have a supervisor or regulator, why is the field "Your institution a Supervised Financial Institution" field is set to "YES" in the KYC-SA application?
A: In the KYC-SA application, the regulator field is prepopulated based on the legal agreement between your BIC and SWIFT. A BIC is classified as 'supervised financial institution' based on the following rules:

1. an entity that engages in payment, securities, banking, financial, insurance, or investment services or activities, and that, for such purposes a. is
   1. licensed by or
   2. authorised by or
   3. registered with a Financial Market Regulator, and is subject to supervision by a Financial Market Regulator as per Resolution 199 (see section 2.2.3.2) or
2. an international, supranational, intergovernmental or national governmental body or institution that as a main activity engages in payment, securities, banking, financial, insurance, or investment services or activities (including central banks).

If you want to update your supervisor or regulator, please create a Support case.

During my attestation I get a warning message that states: "Value differs from SWIFT records, … You can submit different values. SWIFT might contact you for further information." What should I do?
A: In rare/special cases, the prepopulated info in the KYC-SA application can differ from your input due to the use of more than one connection type, different back-up solutions etc. Please check the decision tree and your licence agreements with SWIFT. If you are sure about the information you are providing, you can continue the attestation process disregarding the prepopulated info. In cases where you continue and submit the attestation overwriting the prepopulated info, your attestation will be manually reviewed. If the information you have provided is consistent, SWIFT records will be updated and the attestation will be published.

Back to Index

© 2021 SWIFT

Date of revision	Section impacted	Details	Remark
14 January 2020	Clarifying in section 1.1 the controls applied on archive server hosting sensitive data.	Outlining the options to protect sensitive data stored outside SWIFT secure zone.	
19 March 2020	Generic section	In the context of Covid-19, the relevant controls regarding the remote working options using General Operator PC is clarified.	
27 April 2020	Generic section	Added GPI Tracker access options and relevant architecture types and controls.	
13 May 2020	2.4A Back-office Data Flow Security	New question.	
3 June 2020	Typo in the L2BA question in control 4.2 New question in "Generic" section for middleware.		
17 June 2020	New question in control 2.7	New question in "Control 2.7 Vulnerablity Scanning" section	
18 August 2020	1.3A Virtualisation Platform Protection	Updated answer related to containers in "1.3A Virtualisation Platform Protection" section.	
18 August 2020	Generic section (timelines)	Added link to the Tip 5024006	
21 October 2020	1.1 SWIFT Environment Protection	New topic on Mainframes	

© 2021 SWIFT

29 October 2020	Generic section	New topic on Alliance Warehouse (AWH)
18 November 2020	Generic section	CSCF v2021 - Table with controls per architecture type
18 November 2020	Attachment	Document with full size images for this TIP
9 December 2020	6.4 Logging and Monitoring	New topic on GPI tracker
17 December 2020	Generic section	Only use a Middleware/FTP client to Middleware/FTP server connection
3 March 2021	Generic section	I am using a hosted database, which controls apply to the hosted database and the supporting server?
29 June 2021	1.4 Restriction of Internet Access	How can I comply with the CSP control 1.4 Restriction of internet access when using General Purpose Operator PC (Fully managed or unmanaged device)?
12 July 2021	1.3 Virtualisation Platform Protection	How do I attest if I don't have a virtualization platform?

Back to Last revision Back to Index

Attachment

tip5021823_full_size_images_v1.docx

© 2021 SWIFT