SWIFT Customer Security Controls Framework v2022

Customer Security Programme

Detailed Description

This document establishes a set of mandatory and advisory security controls for the operating environment of SWIFT users. Mandatory security controls build on existing guidance and establish a security baseline for the entire user community. Advisory controls are optional best practices that SWIFT recommends each user to implement in the operating environment. This document must be read in conjunction with the CSP FAQ SWIFT Knowledge Base article 5021823 which provides additional valuable information.

01 July 2021

Table of Contents

Executive Summary

Launched in 2016 in response to the sophisticated cyber attacks on SWIFT users, the Customer Security Programme (CSP) seeks to pragmatically 'raise the bar' of cyber-security hygiene across all users, reduce the risk of cyber attacks and minimise the financial impact of fraudulent transactions. ~~The cyber threat that faces the financial sector has never been greater.~~ There has been a continued evolution since 2016, with SWIFT users facing attacks of increasing levels of sophistication. Modus operandi, the Tactics, Techniques, and Procedures (TTPs) have progressed and changed as institutions strengthen security measures. The persistence of such threats emphasises the importance of remaining vigilant and proactive in the long term. While users are responsible for protecting their own environments and accesses to SWIFT, the ~~Customer Security Programme (~~CSP~~)~~ has been introduced to support customers and drive industry-wide collaboration in the fight against cyber fraud. The CSP establishes a common set of security controls known as the Customer Security Controls Framework (CSCF) which is designed to help customers to secure local environments and to foster a more secure financial ecosystem.

The SWIFT CSCF consists of both mandatory and advisory security controls which are based on industry-standard frameworks, such as NIST, ISO 27000 and PCI-DSS~~for SWIFT users~~. Mandatory security controls establish a security baseline for the entire community and must be implemented by all users on local SWIFT infrastructure. SWIFT prioritises the mandatory controls to set a realistic goal for short-term, tangible security gains, as well as risk reduction. Advisory controls are based on best practices that SWIFT recommends users to implement. Gradually over time, the mandatory controls may change through the evolving threat landscape, and some advisory controls may become mandatory.

SWIFT details all controls around the following three overarching objectives:

- secure your environment
- know and limit access
- detect and respond

The controls have been developed based on SWIFT's analysis of cyber-threat intelligence and in conjunction with industry expert and user feedback. The control definitions are also intended to align with existing information security industry standards.

The controls detailed in this document represent general product-agnostic controls. The controls should not be considered exhaustive or all-inclusive, and do not replace a well-structured security and risk framework that covers the end-to-end transaction chain, sound judgement, or compliance with the latest security best practices.

Given the evolving nature of cyber threats, the introduction of new technologies, and updated SWIFT strategic initiatives, controls will be regularly assessed, refined, and expanded with the changes published in new versions of this document. Consequently, SWIFT recommends users to always consult the latest version of this document through the SWIFT Knowledge Centre (KC).

To support the adoption of the security controls, SWIFT has developed a process that requires users to attest compliance against the mandatory (and optional advisory) security controls. SWIFT requests users to submit an attestation into the KYC Security Attestation (KYC-SA) application. By the end of each year, users must attest compliance against the mandatory (and optional advisory) security controls as documented in the CSCF effective at that time. Generally, a new version of the CSCF is published in July, listing the mandatory and advisory controls users must attest against (as of July of the following year when implemented in the KYC-SA). That is, users must attest between July 2022~~1~~ and December 2022~~1~~ against the security controls listed in the CSCF v2022~~1~~ published in mid-2021~~0~~.

~~As previously communicated to the SWIFT community, SWIFT has re-phased the originally published timelines for the CSCF to make sure upcoming reinforcements are practical for the community. Users must re-attest against CSCF v2019 by the end of 2020. Controls previously detailed in CSCF v2020 are included in CSCF v2021, and users must attest against that framework in the second half of 2021.~~

All users retain control over their own data and are able to grant (automatically or not) access to allow counterparties to view their attestation data. This fosters transparency and creates peer-driven momentum to improve security practices by allowing other users on the network to apply risk-based decision-making efforts concerning their business relationships. For more information about the attestation and reporting process, see the *SWIFT Customer Security Controls Policy (available in* KC*)*.

The CSP is designed to be a collaborative effort between SWIFT and the users to strengthen the overall security of the financial ecosystem. As part of the CSCF Controls change management process, extensive consultation has been undertaken with the community. A new CSCF Working Group has been established, structured around 23 NMGs who positively answered to the initial consultation request. The role of the CSCF Working Group was to centralise, prioritise and review all formal and informal feedback from the community and then finalise the recommended changes. These Working Group sessions were supplemented with SWIFT Oversight work-session calls to ensure transparency with SWIFT Oversight. Therefore, all users must read the controls set out in this document carefully, and prepare their own organisation for implementation accordingly.

Overview of changes

The SWIFT Customer Security Controls Framework (CSCF) version 20222~~1~~ builds incrementally on last year's version (CSCF v2021~~0~~). The CSCF Working Group reviewed several possible 'Change Requests' (CRs), including scope changes, guidance clarifications, cosmetic changes and open questions.

As a result of the consultation and at request of the SWIFT Oversight, CSCF v2022 *promotes* to **mandatory**, after clarification of the scope and the existing implementation guidelines, **Control 2.9 (transaction Business Controls)**. It supports and aligns with other regulations such as CPMI's strategy which equally aims at reducing the risk of payment fraud related to endpoint security. It also recognises the effectiveness of such control in reducing fraudulent financial losses within the community.

A **new advisory control 1.5A (Customer Environment Protection)** is also created to ensure protection of the 'customer connector' and other customer-related equipment by aligning the new control applicable for architecture A4 with the existing control 1.1 already applicable to the other architecture A types.

After the introduction of the **customer connectors** in CSCF v2021 as advisory component in-scope of numerous controls, such components **are** now **fully considered as in-scope** of those controls. **In addition**, to further align with the other architecture A types, **control 6.2 (Software Integrity) and 6.3 (Database Integrity)** are turned as **Advisory for architecture A4**.

To provide basic security hygiene on end-user devices, the **scope of** the existing **control 1.2 (Operating System Privileged Account Control)** is **extended**, **in an advisory way**, to general-purpose operator PCs and as such to architecture B as well.

~~Compared to CSCF v2020, the changes are minimal to make sure the community has enough time to fully implement the controls from previous CSCF versions.~~

~~On paper, CSCF v2021 *promotes* one control to **mandatory.** However, in practice, control **1.4 - Restrict Internet Access**, was already a part of mandatory control **1.1 - Environment Protection / Network Separation** since the launch of the original security controls in 2017.~~

~~In addition, a number of guidelines and scope definitions (primarily for *connectors*) have been clarified to better support attestations and assessments. Moreover, SWIFT has introduced a new architecture type identified as **A4** (which copes with the non-SWIFT footprint). Its introduction gradually supports technology usage resulting from SWIFT's strategy (such as Cloud and APIs) and paves the way for the future, though initially in an advisory way.~~

Further minor clarifications or changes have been made to specific controls or to the overall CSCF framework to improve the usability and comprehension of the document and help users implement the framework as intended:

- Split the 'Security Controls Summary Table' per architecture type: point to a document presenting the relevant controls per in-scope components
- Align wording for in-scope components through the various controls
- Clarify Alliance Gateway Interactive (AGI) Model and update architecture A1 graphics
- Clarify notion of 'test systems' based on the FAQ
- Clarify architecture graphics to differentiate between internal data exchange and external connectivity
- Clarify SWIFT-related component and system definitions
- Control 1.5 - Clarify 'Secure Zones' to support the new control
- Control 2.1 - Move the interactive flows to/from jump servers in Control 2.6 for consistency
- Control 2.4A - Remove redundant references to customer connector
- Control 2.7 - Explicitly refer to network devices as in-scope components
- Control 2.8 - Consistently use the term 'critical activities'

- Control 4.1 - Retrofit latest development (in TIPs) regarding PIN policy for consistency
- Control 4.2 - Incorporate Timed One-Time Passwords (TOTP) and soft tokens as possible Multi-Factor Authentication (MFA) options to align with reality
- Control 5.1 - Ensure accountability and traceability of (re)assigned and delegated accounts; explicitly refer to network devices
- Control 5.2 - Explicitly refer to non-connected tokens
- Control 5.3 - Align control objective with the requested recurring staff screening
- Control 6.4 - Provide guidance on global log retention to support forensics in line with local legislation
- Control 7.1 - Consider SWIFT recovery roadmap as a guide, not as a prescribed approach
- Control 7.2 - Split 'annual security awareness' expectation from 'maintaining knowledge over time'

SWIFT recommends users to consult the *CSCF v2022 compared to v2021* version of this document to view the full detail of all related changes. This does not include editorial changes that SWIFT makes to improve the readability of the document.

~~and highlight expectations on the usual initial cyber targets: the general operator PCs that connect to local or remote infrastructures.~~

~~Some suggested implementations have also been incorporated (for more information, see controls **1.1**, **2.9A**, **6.1**, **6.5A**, and **7.4**).~~

~~To enhance efficiency and to make sure of the continuous identification of components within the controls' scope, an initial list is proposed in **Appendix F**. SWIFT will regularly update this list.~~

To further ease independent assessments, SWIFT reminds users of the following:

- Compliance with control objectives is a risk-based approach. The provided implementation guidelines can be used as a starting point, but cannot be considered as strict audit checklists.
- Users engaging with third parties (including cloud providers) to host or operate (in full or in part) their own SWIFT infrastructure must obtain reasonable comfort from third parties that the outsourced activities or externally hosted components are protected per the security controls. As such, third parties can rely on their compliance programme that usually builds on SOC 2, PCI-DSS or NIST certifications or assurance to answer users engaging with them and map the CSCF security controls. For example, **Appendix G** presents the shared responsibilities when moving to an Infrastructure as a Service (IaaS) model in the cloud.

~~The following table summarises the most significant changes to the content of this document compared to the previous version. The table does not include editorial changes that SWIFT makes to improve the usability and comprehension of the document. SWIFT recommends users to consult the CSCF v2021 compared to v2020 version of this document to view the full detail of all related changes.~~

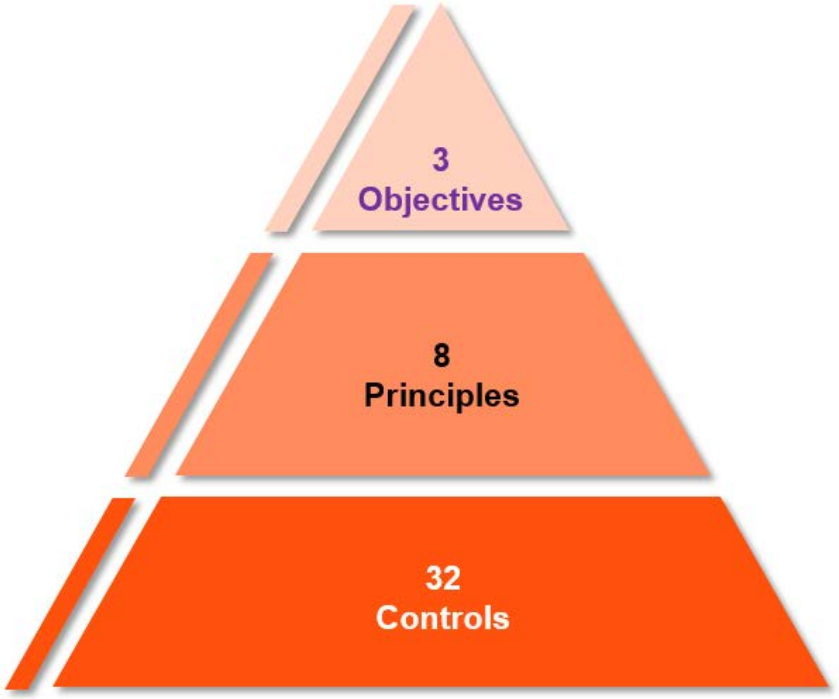
~~Control or section~~	~~Change~~
~~**Confirm split of existing controls for efficiency**~~	
~~Further strip down control 1.1 by transferring Restriction of Internet Access to the control 1.4~~	~~Centralise in control 1.4 the guidance related to internet access and removed the latter from 1.1 d) and e)~~
~~**Clarifications on scope definitions and new architecture - Alignment to reality and new models**~~	
~~Connector definition~~	~~Embed middleware/MQ servers and API end points when used to connect or transmit transactions to service providers or SWIFT~~

Control or section	Change
	Differentiate SWIFT-related connectors (such as SIL, DirectLink, AutoCLient, MicroGateway) from customer connectors (based on file servers, middleware/MQ servers or custom-made API end-points)
General Purpose Operator PCs	Clarified that accessed infrastructures or applications can be locally or externally hosted/operated Explicit reference to general purpose operator PC in the relevant controls and clarifications to support appropriate implementation when it matters
Third party	Extended to cloud provider It is reminded that when engaging with a third party, users remain responsible for securing their infrastructure and have to obtain reasonable comfort from third parties that the outsourced activities or externally hosted components, or both are protected as per the CSP security controls Appendix G added to illustrate when outsourcing using an IaaS model
Architecture Types – Architecture A4	A new Architecture Type is introduced to differentiate users relying on SWIFT connectors (or SWIFT footprint), currently designated as A3, from those relying on customer connectors (no SWIFT footprint), new A4 Previous scope extension to middleware/MQ servers and the repositioning of the file server solutions as customer connector might require some existing B or A3 architectures to become A4
Security Controls Compliance – Support of the independent assessments	
Security Controls Compliance and on each control	It is reminded that implementation guidelines are not strict audit check lists but are to be assessed using a risk-based approach
Clarifications to existing controls for efficiency and alignment to reality	
1.1 SWIFT Environment Protection	Inclusion of temporary access as a potential alternative to different jump servers for users and admin connection to secure zone
1.3 Virtualisation Platform Protection and related controls	Explicit reference to remote (externally hosted or operated) virtualisation platform to foster attention when engaging with a third party or moving to the cloud
2.4A Back Office Data Flow Security and related controls	Newly introduced customer connectors treated similarly to the local middleware/MQ servers: in scope extension for some controls (advisory when used)
2.7 Vulnerability Scanning	Advisory for architecture B (that is, only an optional enhancement for general purpose operator PCs)
2.8A Critical Activity Outsourcing	Reminds the user responsibility when engaging with a third party or a service provider
2.9A Transaction Business Controls	24/7 operational environment taken into account and suggested implementation

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

Framework Objectives and Principles

Objectives and Principles



The security controls are based on three overarching framework objectives, supported by eight security principles. Objectives are the highest level structure for security within the user's local environment. The associated principles elaborate on the highest priority focus areas within each objective. The objectives and corresponding principles include the following:

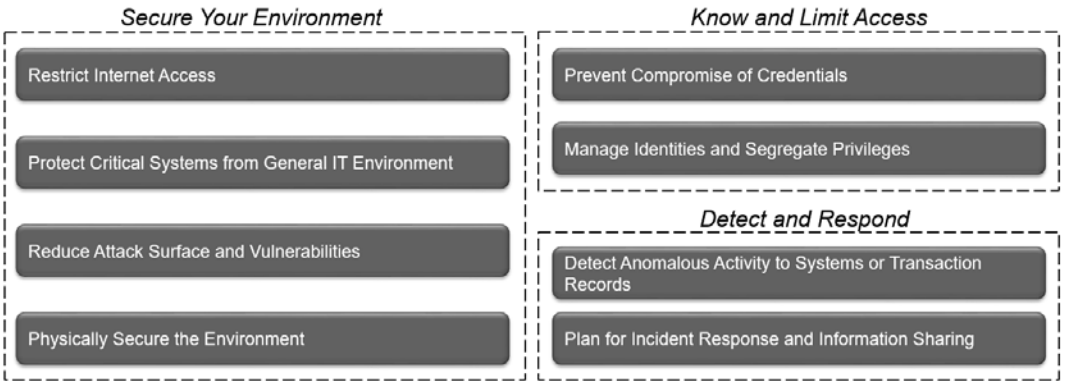


Figure 1: Framework Objectives and Principles

The 321 security controls (232 mandatory controls and 9 advisory controls) detailed in this document underpin these objectives and principles where the first two principles, sharing common controls, have been grouped. The controls help mitigate specific cyber-security risks that SWIFT users face due to the cyber-threat landscape. Within each security control, SWIFT has documented the most common risk drivers that the control is designed to help mitigate. Addressing these risks aims to prevent or minimise undesirable and potentially fraudulent business consequences, such as the following:

- unauthorised sending or modification of financial transactions
- processing of altered or unauthorised SWIFT inbound transactions (that is, received transactions)
- business conducted with an unauthorised counterparty

- confidentiality breach (of business data, computer systems, or operator details)
- integrity breach (of business data, computer systems, or operator details)

Ultimately, these consequences represent enterprise-level risks, including the following:

- Financial Risk
- Legal Risk
- Regulatory Risk
- Reputational Risk

Integration with Security Governance and Risk Management

SWIFT encourages users to consider cyber risk management in the broadest possible terms, including beyond the scope of the user's SWIFT infrastructure and the SWIFT security controls. For the most effective management of risk, users should not view the implementation of these security controls as a one-time activity, nor as exhaustive or all-inclusive. Users should, instead, incorporate SWIFT's controls into an ongoing cyber-security governance and risk programme within their organisation, considering sound judgement and the latest best practices, taking into account user-specific infrastructure and configurations. As a result, users can re-use and benefit from existing policies, procedures, and controls that have been established to manage other areas of cyber risk. To help users in this approach, **Appendix E** contains a mapping of the SWIFT security controls against three international security standard frameworks: **NIST Cybersecurity Framework v1.1**, **ISO 27002 (2013)**, and **PCI-DSS 3.2.1**. SWIFT has also published a guiding document to assist users in assessing counterparty cyber-security risk and incorporating this into the risk management framework.

A holistic approach to cyber risk is most effective in avoiding enterprise-level risk, therefore improving the overall safety of each individual organisation and the wider financial community.

Additionally, users should have the correct level of accountability and oversight for their cyber risk management activities. Generally, a Chief Information Security Officer plays a prominent role in this domain by directing the priorities of the security programme and soliciting the appropriate support and guidance from the Board.

Scope of Security Controls

The scope of security controls in this document encompasses a defined set of components in the user's local environment (see Figure 2).

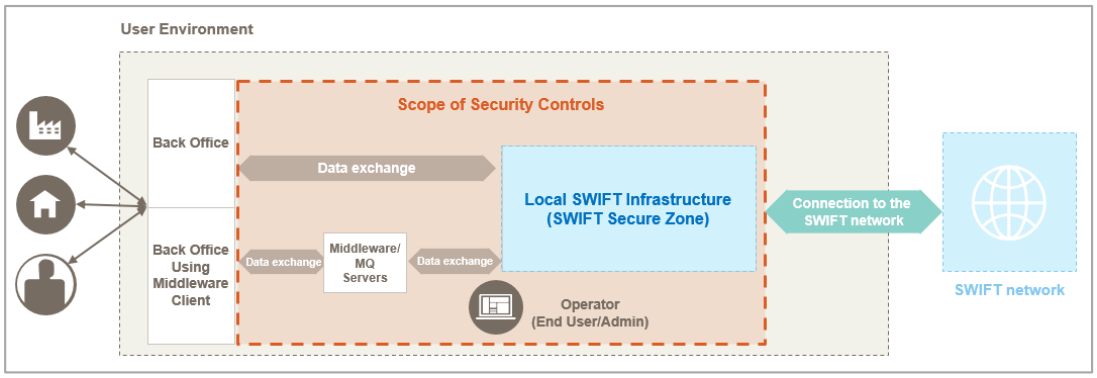


Figure 2: Scope of Security Controls

The security controls apply to the following in-scope components:

- **Local SWIFT infrastructure –** The collection of, on premises or externally hosted, SWIFT-specific components managed by or for users, including applications, network devices~~components~~, tokens and other removable media, and supporting hardware. Examples of local SWIFT infrastructure set-up and so called SWIFT-related components (depending on the user architecture type) are as follows:
  - **SWIFT Secure Zone**: a segmented zone that separates SWIFT-related systems from the wider enterprise environment (further detailed in control 1.1). This zone can expand beyond the local SWIFT infrastructure and can include non-SWIFT systems. Its primary purpose is to host the below identified SWIFT footprints.
  - **Messaging Interface**: a ~~Messaging Interface~~ software that supports the use of MT, MX, or ISO 20022 message standards through SWIFT FIN, InterAct, FileAct, and SWIFTNet Instant messaging services. The software provides the means for users to connect these business applications to SWIFT messaging services and is typically connected directly to the communication interface. SWIFT provides messaging interfaces (for example, Alliance Access and Alliance Messaging Hub or Alliance Messaging Hub Instant). Messaging interfaces that hold a SWIFT-compatible label can also be provided by third-party vendors. A Messaging Interface is considered as a SWIFT footprint.
  - **Communication Interface**: a ~~Communication Interface~~ software that provides a link between the SWIFTNet network and usually* the Messaging Interface software or a back-office system. Communication interfaces provide centralised, automated, and high-throughput integrations with different in-house financial applications and service-specific interfaces. SWIFT provides the communication Interfaces (for example, Alliance Gateway or Alliance Gateway Instant). Communication interfaces that hold a SWIFT-compatible label can also be provided by third-party vendors. A Communication Interface is considered as a SWIFT footprint. * While Alliance Gateway is usually linked with a Messaging Interface, Alliance Gateway Instant is usually directly linked with a back-office system (unless an explicit Messaging Interface is also integrated in the user infrastructure).
  - **SWIFTNet Link (SNL)**: SNL is a mandatory software product for access to FIN, InterAct, and FileAct messaging services over a secure IP network. This document refers to the SNL, a SWIFT footprint, as part of the Communication Interface scope.
  - **Connector**: Connectors are local software designed to facilitate communication with an external messaging interface or a communication interface (or both), or to a service provider (handling as such the external connection). When using a

connector, interface components are usually offered by a service provider (for example, offered by a service bureau, a hub infrastructure, or SWIFT).

SWIFT connector is a connector specifically designed to support SWIFT business. It is usually provided by SWIFT (for example, Alliance Cloud SIL, Direct Link, Alliance Lite2 AutoClient, in combination with SIL or not in combination with SIL, or Microgateway). SWIFT connector, holding a SWIFT-compatible label, can ~~potentially~~ also be provided by third-party vendors. A SWIFT connector is considered as a SWIFT footprint.

Customer connector is typically a commercial off-the-shelf product configured for SWIFT purposes. It includes generic file transfer solutions or local middleware systems implementations (such as IBM® MQ server) used to facilitate ~~communication~~ an external connection with SWIFT-related components offered by a service provider. Those generic elements not provided by SWIFT (or not labelled as SWIFT-compatible) are considered as a non-SWIFT footprint.

In the future, an application developed in-house that implements SWIFT APIs (either using the specifications or integrating the SWIFT SDK) to connect and transmit business transactions independently[1] to SWIFT messaging services[2] exposed by the SWIFT API Gateway, will also be considered as a customer (bespoke API) connector or a non-SWIFT footprint.

The term ***connector*** alone refers to both SWIFT connectors and customer connectors.

- **Customer Secure Zone**: a secure operational (sometime also called production) environment that separates non-SWIFT footprint, such as the customer connector, from the wider enterprise environment (further detailed in control 1.5). Its primary purpose is to host the customer connector but can also include non-SWIFT related systems which then also need to be adequately protected. Users already having a SWIFT secure zone may consider adding in that zone a customer connector (in which case there is no need to create a specific customer secure zone for the latter). Note: a customer secure zone can also host systems supporting an existing SWIFT secure zone such as a storage area network (SAN), a hosted database, a virtualisation platform, authentication services or middleware servers.

  Secure zone: refers to a SWIFT or a customer secure zone.

- SWIFT Hardware Security Modules (HSMs), connected and disconnected personal tokens, and smart-cards.

- Firewalls, switches, and routers within or surrounding the SWIFT infrastructure (dedicated or shared) referred to generically as network devices protecting the secure zone.

- **Graphical user interface (GUI)**: software that produces the graphical interface for a messaging interface, a communication interface or a connector~~a user~~ (for example, Alliance Web Platform Server-Embedded, SWIFT Microgateway Front-End, and equivalent products).

- **Operators**: Operators are individual end users and administrators that directly interact with the ~~local~~ SWIFT infrastructure at the application or OS level.
- **Operator PCs:** the end user's or administrator's computing device (typically a desktop or laptop) used to conduct their duties as an operator (to use, operate, or maintain the local SWIFT infrastructure residing on premises or externally hosted) or as a user (to use a remote SWIFT infrastructure or application operated by a service provider, such as a service bureau, a Lite2 for Business Application provider, an intermediate actor, a Group Hub or SWIFT), or a combination, depending on the architecture type.

[1] Independently means without using a communication interface or a SWIFT connector such as SIL, Direct Link or Microgateway

[2] Business transactions to messaging services refers to requests introducing or affecting SWIFT payments (such as creation of MT103, 101, 202, 205 or cancelling/stopping/recalling/modifying those requests). On the other side, queries on previous transactions (such as through the Basic Tracker), prevalidation, conversion or screening performed before submitting business transactions are not considered affecting messaging services and can be considered as out of scope unless they require the same roles/entitlements as business transactions to messaging services (no ~~segregation~~ separation of duties and precautionary principle has to be applied).

A ***general-purpose operator PC*** is generally located in the general enterprise IT environment and is used for daily business activities including accessing the local or a remote SWIFT infrastructure or an application operated by a service provider, depending on the architecture type. It also includes devices (physical or virtual desktop, laptops but also other devices such as tablets or mobiles) managed by the customer and used to interact with the messaging or communication interface, a GUI, a connector or a service provider SWIFT-related application.

A ***dedicated operator PC*** is located in the secure zone and is dedicated to interact with components of the secure zone (sometimes also referred to as an *operational console*).

The term ***operator PC*** alone refers to both general-purpose and dedicated operator PCs.

- **Data exchange layer:** the transport of data between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and a user back-office first hop, at application level, as seen from the SWIFT-related components.
- **Middleware server:** local middleware systems implementations, such as the IBM® MQ server (including MQ queues manager, MQ appliance, or both), used for data exchange between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office. It must be considered as a customer connector when used to facilitate ~~communication~~ an external connection with SWIFT-related components offered by a service provider (such as a service bureau, or potentially a Lite2 for Business Application provider).

The following components are out of scope:

- **User back-office:** the systems responsible for business logic, (financial) transaction generation, and other activities that occur before transmission into the local SWIFT infrastructure. For example:
  - Back-office implementations such as SAP, General Ledger, or applications that use an MQ Client to liaise with a SWIFT infrastructure are out of scope unless co-hosted with an in-scope component.
  - An application or system relying on a communication interface, such as Alliance Gateway (see Figure 3b) or a SWIFT connector, such as Direct Link or Microgateway (see Figure 5) or, in the future, a customer connector (see Figure 6b) for API calls to SWIFT remains a back-office and is out of scope unless co-hosted with the communication interface or the connector.
- **General Enterprise IT environment:** the general IT infrastructure used to support the broader organisation (for example, general-purpose PCs, mail servers, or directory services).

Connections to the SWIFT network supplied by SWIFT Network Partners and~~,~~ Internet connections to the SWIFT network~~, and Alliance Connect SRX VPN boxes (or the virtual instances) remotely managed by SWIFT~~ are also out of scope. **However**, the remotely managed by SWIFT Alliance Connect SRX VPN boxes and the upcoming Alliance Connect V~~v~~irtual VPN instances[3] (hosting systems or machines) are in scope of control **3.1** (expected to be in an environment with appropriate physical controls~~) in line with the control **3.1**~~. **In addition**, the virtualisation platform hosting Alliance Connect Virtual VPN instances, is also in scope of the control **1.3**.

Although it is not mandatory for the purposes of the attestation process, the security controls reflect security best practices and it is appropriate to implement them beyond the in-scope environment into the broader end-to-end transaction chain.

Note: **Users must attest** for all in-scope components in the local live, back-up, and disaster recovery environment, while **taking into account the** specific but still **comprehensive architecture** (**declaring the most**

[3] Also called v SRX

encompassing architecture type that can also be identified using the decision tree).

~~As such, test systems are preferably fully separated from production systems (including separate HSMs) and configured to only support test traffic (for example, by only using lite certificates and only configuring test logical terminals).~~ Test systems are not considered in scope of the security controls as long as (i) they are fully separated from production or live environment (including separate HSMs) and (ii) they are configured to only support test traffic (for example, by only using lite certificates on test only logical terminals). If the test systems are not fully separated or can be configured for live traffic, then users must take the test systems in scope and make sure that the same security controls are applied as for production or live systems. ~~If not fully separated, then the systems must be maintained to the same security level as the production systems.~~

Similar to the back-office, users should still implement good security hygiene on their test systems to also make sure they cannot be easily reconfigured for live traffic.

Development systems are not within the secure zone and are not connected to the SWIFT network.

The primary purpose of a secure zone is to host SWIFT-related components but it can also include non-SWIFT related systems as long as they are adequately protected. All components within the secure zone must be protected to an equivalent level of security and trust by applying controls applicable to the SWIFT-related components (see the CSP FAQ for the relevant controls).

Similarly, the purpose of a SWIFT-related system is to host or run a SWIFT-related component turning such system and co-hosted (running on that system) applications in scope, irrespective on the underlying layer (individual/physical host, virtual machine on a virtualisation platform or deployed in the Cloud). The virtualisation platform must also be specifically considered and deployment in the Cloud is simply an abstraction of the virtualisation platform and similar approach has to be sought in line with below note.

Appendix F supports the identification of elements or SWIFT-related components in-scope.

Note: Users that engage with third parties (for example, an external IT provider or a cloud provider) or service providers (such as a service bureau or a Lite2 for Business Application provider which, in this specific case, must be considered as a third party) to host or operate in full or in part the user's SWIFT infrastructure must be aware of the following:

- Users are still responsible and accountable to attest for their comprehensive architecture type (as if it was operated on premises).
- Consequently, users must get reasonable comfort[4] from such third parties or service providers that the related activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation and in line with the CSCF security controls. As such, third parties can rely on their compliance programme that usually builds on SOC 2, PCI-DSS or NIST certifications or assurance to answer users engaging with them.

Appendix G illustrates a typical spread and share of responsibilities to consider when outsourcing to a cloud provider through an Infrastructure as a Service (IaaS) model.

[4] See the Glossary of Terms for the definition

Architecture Types

Each user must identify which of the five reference architecture types (Figures 3-7) most closely matches their own architecture deployment to determine which components are in scope (a CSP architecture decision tree is available). Depending on the architecture type where the most comprehensive one has to be chosen, some security controls may or may not apply.

The five reference architectures are as follows, where component or licence ownership is the key differentiator:

- **Architecture A1** – Users owning the communication interface (and, generally, the messaging interface)

  The communication interface is owned by the user.

  Figure 3a displays the case where both the messaging interface and the communication interface licences are owned by the user and reside within the environment.

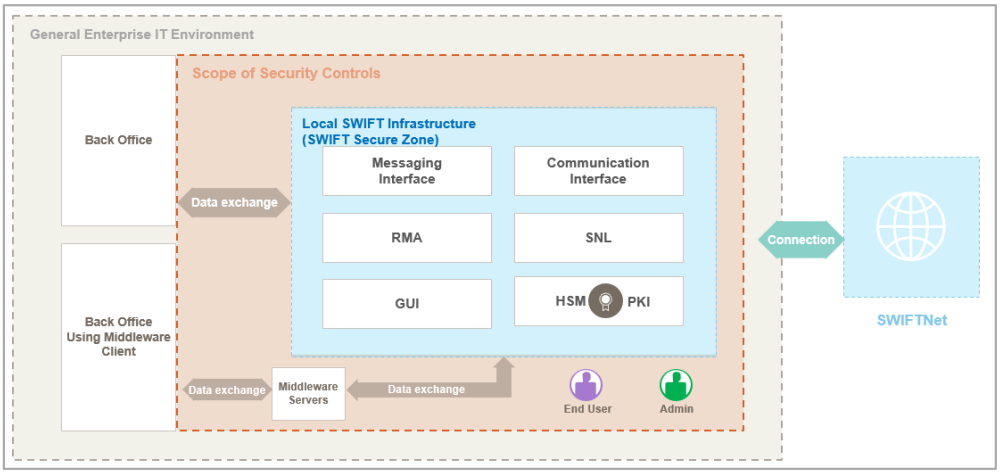


Figure 3a: Architecture A1 – Interfaces within the user environment

Users that do not own a messaging interface but only own a communication interface (such as in the Figure 3b below) are also considered as **architecture A1**.

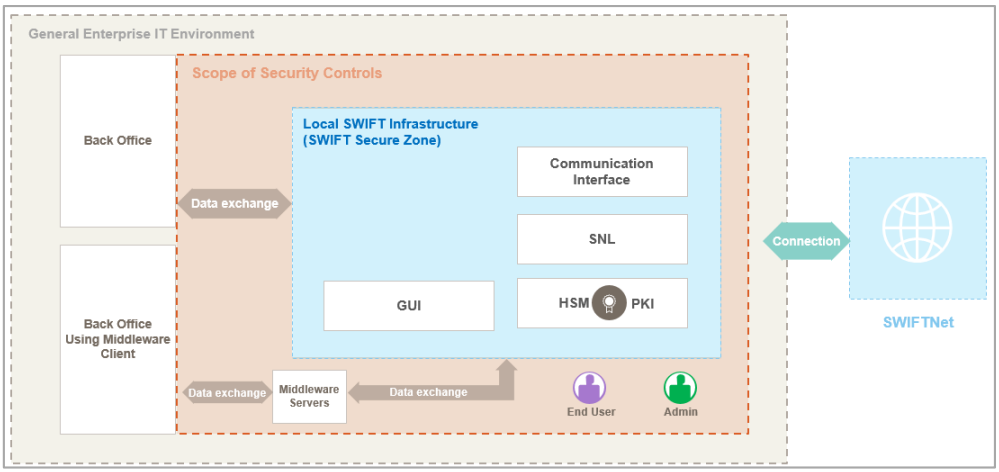


Figure 3b: Architecture A1 – Communication interface only within the user environment

The **architecture A1** type also includes hosted solutions where the user owns the licence for the communication interface that the user operates on behalf of other users, or the communication interface owned by the user is operated for personal use by a third party within (or hosted) outside the user environment. An Alliance Gateway Instant linked with a back-office system without any Messaging Interface illustrates such set-up.

- **Architecture A2** – Users owning the messaging interface, but not the communication interface

  The messaging interface is owned, but a service provider (for example, a service bureau, SWIFT[5], or a Group Hub) owns the licence for the communication interface.

  Figure 4 displays the case where the messaging interface is owned by the user and resides within the user environment.

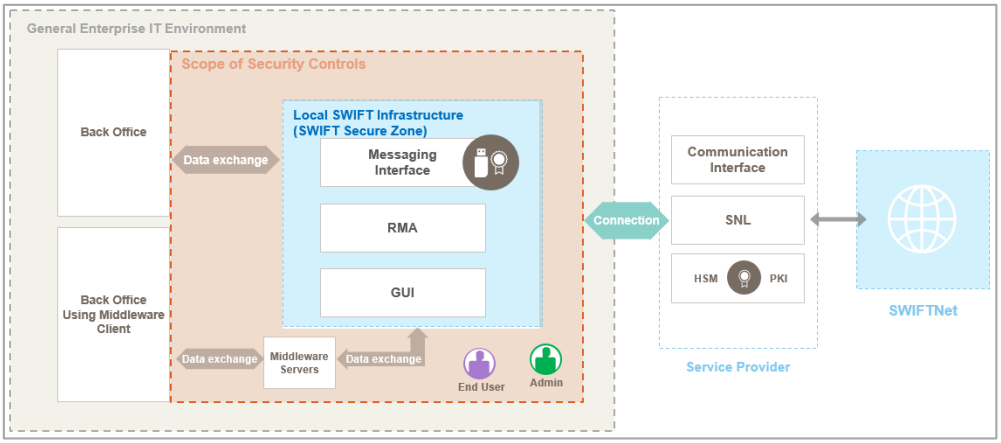


Figure 4: Architecture A2 – Messaging Interface only within the user environment

This architecture type also includes hosted solutions where the user has the licence for the messaging interface that is operated on his behalf by a third party or a service provider.

- **Architecture A3** – SWIFT Connector

  A SWIFT connector[6] is used (such as in Figure 5) within the user environment to facilitate an application-to-application communication with an interface at a service provider (for example, a service bureau or a Group Hub) or with SWIFT services (such as Alliance Cloud or Alliance Lite2) with no interface.

  Optionally, this set-up can be used in combination with a GUI solution (user-to-application). In such cases, controls pertaining to the GUI must also be implemented.

  This architecture type also includes hosted solutions of the SWIFT connector.

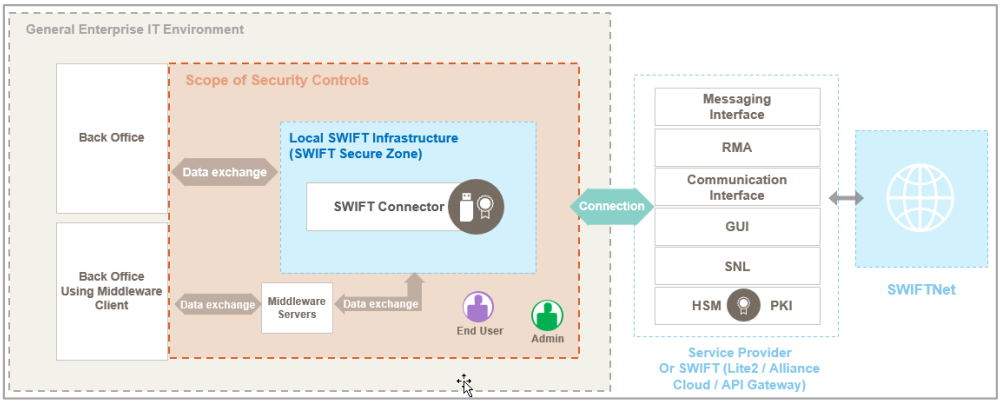


Figure 5: Architecture A3 – SWIFT Connector

- **Architecture A4** – Customer Connector

  A server running a software application (for example, a file transfer solution or a middleware system such as an IBM® MQ server or similar that is a customer

[5] In the scope of Alliance Remote Gateway

[6] For example, Alliance Cloud SIL, Direct Link, Alliance Lite2 AutoClient, in combination with SIL or not, or Microgateway

connector, see Figure 6a) is used within the user environment[7] to facilitate an application-to-application ~~communication~~ external connection with an interface at a service provider (for example, a service bureau, a Lite2 Business Application provider, or a Group Hub) with no SWIFT footprint.

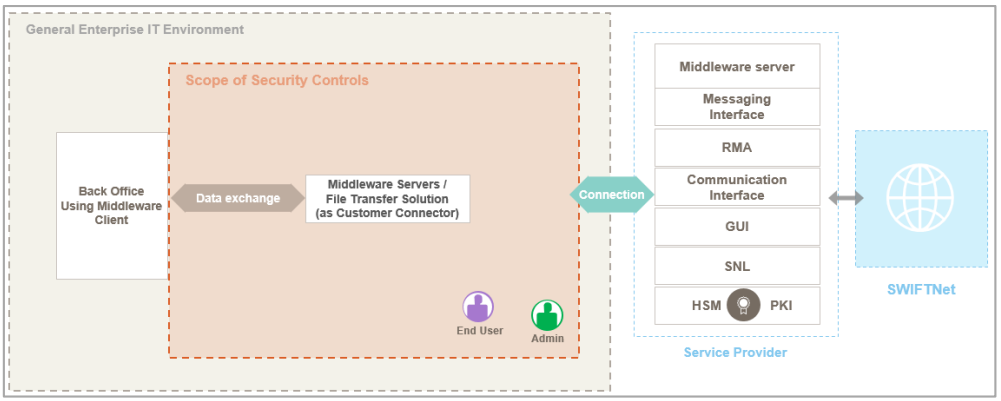


Figure 6a: Architecture A4 – Middleware/File Transfer as Connector

This specific architecture will require the following users to be turned as **Architecture A4**:

- users that previously attested as ~~**B**~~ **Architectures B** when using (as a customer connector) a middleware server, such as an MQ server to connect with a service provider or a Group Hub.

- users that previously attested as ~~**A3**~~ **Architecture A3** when using (as a customer connector) a file transfer solution or a middleware server, such as an MQ server, or both, to connect with a service provider or a Group Hub with no SWIFT connector.

~~The a~~Above users must also consider, for the data exchange with the back office, ~~the~~ controls~~,~~ with~~having~~ an in-scope middleware server ~~in-scope~~.

To pave the way for the future, **Architecture A4** also includes, as customer connectors, ~~as~~ applications used within the user environment[8] that~~to~~ implement SWIFT APIs to directly connect and independently transmit[9] business transactions to SWIFT services (a future messaging service[10] or the Transaction Management Platform[11] exposed by SWIFT) with no SWIFT footprint. The implementation of the SWIFT APIs (using either the specifications or integrating the SWIFT SDK) makes such applications a custom-made API endpoint referred to as a customer connector or a non-SWIFT footprint (see Figure 6b).

This last set-up could also integrate a GUI solution (user-to-application). In such a case, controls relevant to the GUI must be implemented as well.

[7] On premises or externally hosted, in the Cloud or not.

[8] On premises or externally hosted, in the Cloud or not.

[9] Without the usage of a communication interface or a dedicated SWIFT (API) Connector.

[10] Business transactions to messaging services refers to requests introducing or affecting payments (such as creation of MT103, 101, 202, 205 or cancelling/stopping/recalling/modifying those requests). On the other side, queries on previous transactions (such as through the Basic Tracker), prevalidation, conversion or screening performed before submitting business transactions are not considered affecting messaging services.

[11] To be deployed in the future as part of the Board endorsed SWIFT Strategy

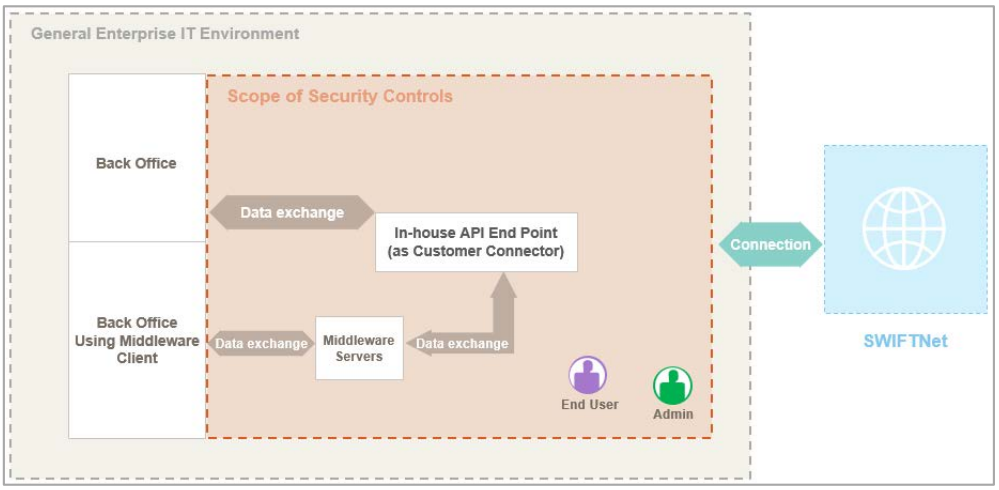


Figure 6b: Architecture A4 – Customer (~~home-made~~in-house API) Connector

- **Architecture B** – No local user footprint

  No SWIFT-specific infrastructure component is used within the user environment. The following two types of set-ups are covered by this architecture type:

  – Users only access SWIFT messaging services through a GUI application at the service provider (user-to-application). The PC or device used by those users to submit or affect business transactions must~~should~~ be considered as a general-purpose operator PC and must~~should~~ be protected accordingly.

  – A user's back-office applications communicate directly with the service provider (application-to-application) using APIs from the service provider or a Middleware client (such as an MQ Client) without connecting or independently transmitting business transactions to ~~SWIFT~~ Alliance Cloud, a SWIFT messaging service, the SWIFT API Gateway[12] or, in the future, the Transaction Management Platform[13] exposed by SWIFT. In such a case, the service provider must make sure that the security of the environment and the security of the data exchange with the user are aligned with the CSCF controls. Categorising this set-up as **Architecture B** is aligned with the scope of the security controls, which excludes user back-office applications. However, SWIFT strongly recommends already implementing **Architecture A4** controls on the applications that integrate APIs or a Middleware client (such as an MQ Client).

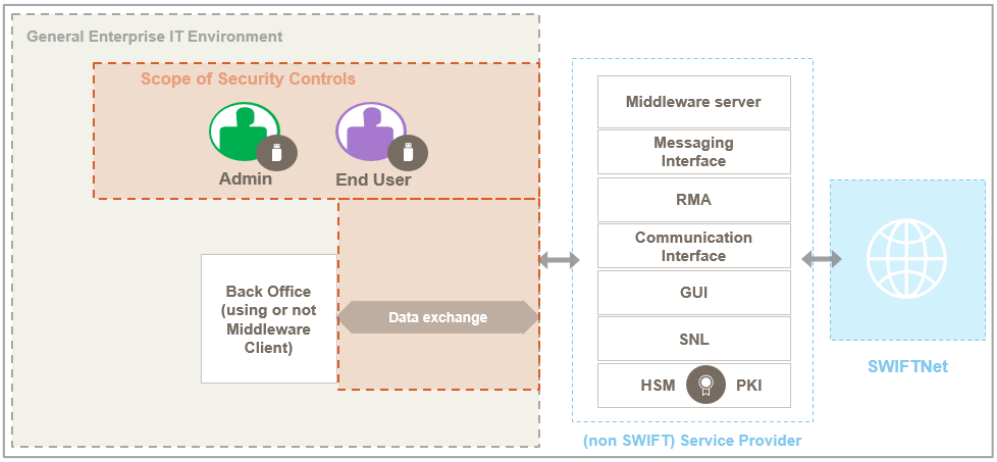


Figure 7: Architecture B - No user footprint connecting to a Service Provider (other than SWIFT)

[12] Would otherwise be considered as an architecture type A4 with a customer connector.

[13] To be deployed in the future as part of the Board endorsed SWIFT Strategy

This architecture type also includes users that only access SWIFT messaging services (user-to-application) with a browser, exposed by Alliance Cloud and Alliance Lite2. PCs used by those users to submit or affect business transactions must be considered as general-purpose operator PCs and must be protected accordingly.

The security controls applicable for **Architectures A1**, **A2**, and **A3** are identical[14] and fewer controls apply to **Architecture A4**. These architectures are referenced collectively on the following pages as type ***A***. Fewer security controls apply to users that utilise Architecture type ***B*** (for more information, see the *Security Controls Summary Table* section).

[14] Except for Control 6.3 Database Integrity that explicitly does not apply to any architecture A3

Security Controls Structure

Each security control in this document is structured into the following three parts:

- general control information
- control definition
- implementation guidance

General Control Information

- **Control Number and Title:** Each control has a unique number and title. If the control number is suffixed with an *A*, then this indicates that the control is *Advisory*.
- **Control Type:** This identifies the control as *Mandatory* or *Advisory*. Users must implement all applicable Mandatory controls, taking into account the architecture type. Advisory controls are considered as a security best practice and are strongly recommended for additional implementation.
- **Applicability to Architecture types**: Controls are applicable either to users with **Architecture types A1**, **A2**, **A3**, **A4**, **type B**, or a combination of types. As such, users with **Architecture type B** are not required to comply with controls applicable to **Architecture types A1**, **A2**, **A3** and **A4** only.

Control Definition

- **Control Objective**: The security goal to be achieved, irrespective of the implementation method.
- **In-scope Components**: The specific SWIFT-related components covered by this particular control. (For more information, see Scope of Security Controls. The Controls_Matrix document can also be consulted to have a view of the relevant controls per in-scope component.)

  Note: When extending the scope to new components, the new in-scope components can initially be tagged as *Advisory*[15].
- **Risk Drivers**: The specific risks addressed by this particular control. A full matrix of risks is documented in Appendix A.

Implementation Guidance

- **Control Statement**: The suggested means by which the Control Objective can be fulfilled.
- **Control Context:** Additional introductory background information about this control.
- **Implementation Guidelines**: The SWIFT-formulated method for control implementation.

Important Users must attest against their compliance with all mandatory control objectives. Additional details about implementation options for compliance are described in the next section. Users can also find additional valuable information in the CSP FAQ (SWIFT Knowledge Base article 5021823) and the Security Guidance Document (log in on swift.com required).

[15] The Change Management process makes sure that the SWIFT community has sufficient time to understand and implement any future changes to the control requirements. Typically, new mandatory controls will be first introduced as advisory, thereby giving all users at least two cycles to plan, budget and implement.

Security Controls Compliance

As per the above-described security controls structure, the objective of a control states the security goal to be achieved irrespective of the implementation method used.

To comply with a CSP security control, users must implement a solution that meets the control definition; namely, the solution~~does the following~~:

- meets the stated control objective
- covers the documented in-scope components relevant for the user's architecture
- addresses the risk drivers (see Appendix A for a risk matrix and Appendix C for illustrations of such risks)

The *Control Statement* is the suggested means to fulfil the control objective and the *Implementation Guidelines* are common methods for implementing the control.

Compliance can be obtained by either of the following methods:

A) Implement a solution aligned with the implementation guidance provided in this document.

The *implementation guidance* section should not be considered as a strict "audit checklist" because each user's implementation can vary. Therefore, in the case that some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be taken into account to properly assess the overall guideline's adherence level.

B) Implement an alternative solution to the SWIFT-formulated implementation guidance, which equally meets the control ~~objective and addresses related outlined risks~~definition.

In such a case, deployed controls, their effectiveness, and particular environment specificities must be taken into account to properly assess the control definition~~objective~~ compliance of the solution (risk assessment approach).

Both methods are considered as valid and equally robust from a risk perspective.

Users are ultimately responsible for assessing the suitability of SWIFT-formulated implementation guidance in their environment or determining if they want to adopt alternative implementation solutions.

It is the expectation that only a small subset of users (typically those with a high level of Information Security Risk Management maturity within their organisation) will consider alternative implementation methods for one or more controls to cope with large or complex configurations.

Security Controls Summary Table

The following table provides an overview of all mandatory and advisory security controls, structured according to the principle they support and with reference to the architecture type to which they relate. In addition, the table identifies the relevance of the controls, depending on the architecture type. Advisory controls are notated with an *A* after the control number (for example, *2.4A*) throughout this document, and are shaded in the table below. Likewise, individual shaded cells in the table below are advisory for some specific architecture types even when the control is mandatory for other architecture types.

Note: ○ identifies the control to be considered for related Architecture types when they have a customer connector in addition to their SWIFT footprint.

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	●	●	●	●	●
1.5A Customer Environment Protection	○	○	○	●	
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	●	●	●	●	●
2.9~~A~~ 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 Se~~gre~~parate~~gate~~ Privileges					
5.1 Logical Access Control	●	●	●	●	●
5.2 Token Management	●	●	●	●	●
5.3A Staff Screening~~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	•	•	•	•	•

The following two figures present visually where the controls would apply using, for reference, one of many ways an **Architecture A1** could be designed. (See *Appendix B* for other reference architectures. The Controls_Matrix document can also be consulted to have a view of the relevant controls per in-scope component.)

Figure 8 shows the controls applied at the infrastructure and hosts level combined with organisational controls surrounding such an environment. Figure 9 shows the interactive or application flow controls between the SWIFT-related components and the operator PCs or back-office systems.

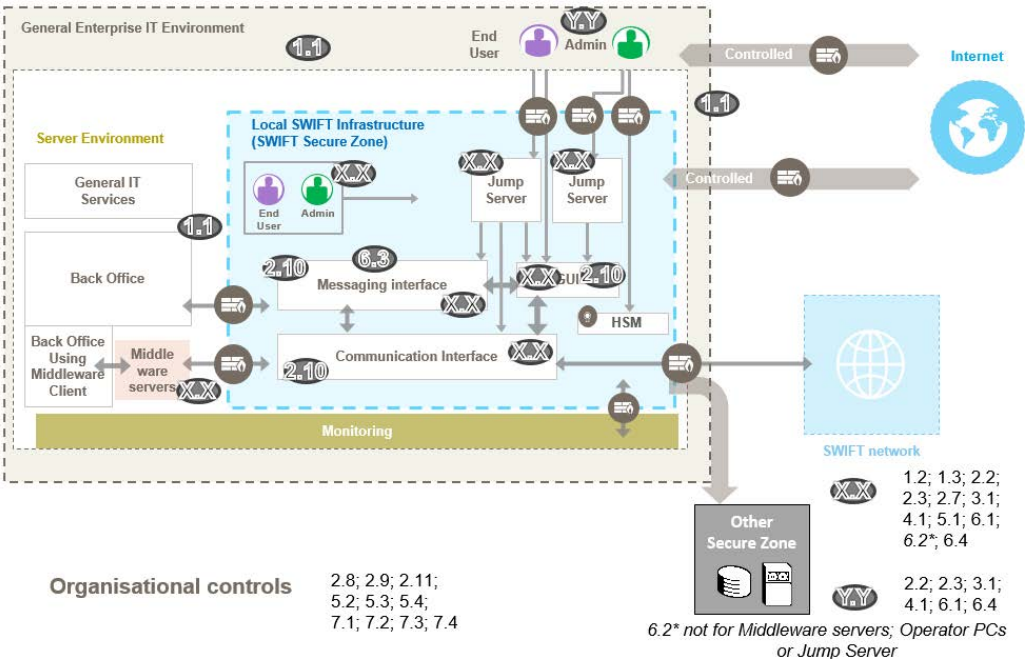


Figure 8: Infrastructure static and organisational controls

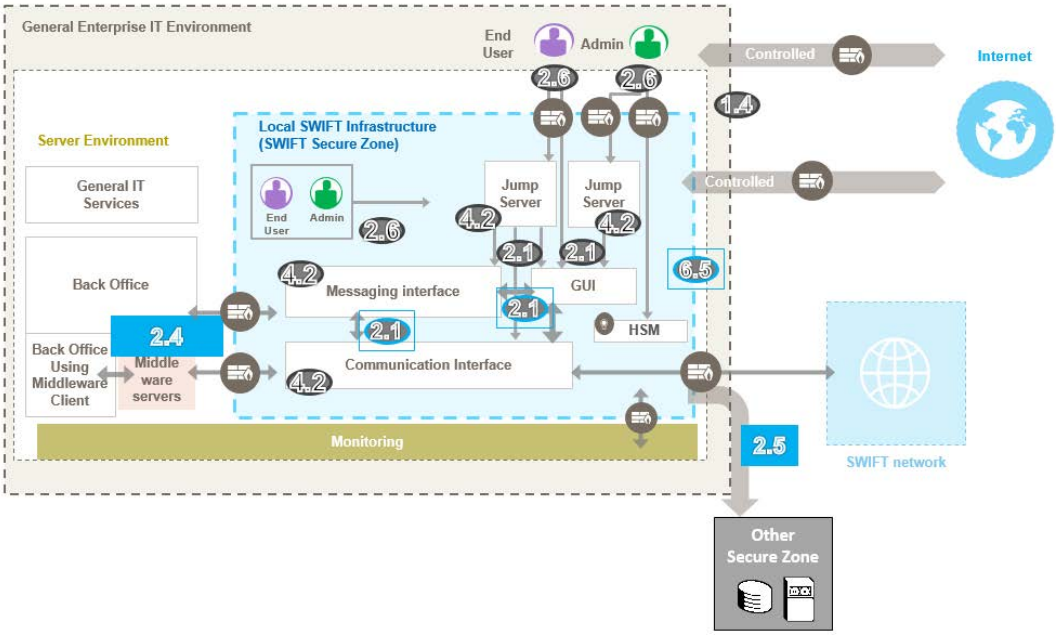


Figure 9: Human/Application to Machine/application flow controls

Detailed Control Descriptions

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

1.1 SWIFT Environment Protection

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•		

Control Definition

Control Objective: Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.

In-scope components:

- messaging interface
- communication interface
- GUI
- SWIFTNet Link
- Hardware Security Module (HSM)
- SWIFT connector
- jump server
- dedicated and general-purpose operator PCs

Risk Drivers:

- compromise of enterprise authentication system
- compromise of user credentials
- credential replay
- exposure to internet-based attacks
- unauthorised access

Implementation Guidance

Control Statement:

A separated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments.

Control Context:

Segmentation between the user's local SWIFT infrastructure and the larger enterprise network reduces the attack surface and has shown to be an effective way to defend against cyber attacks that commonly involve a compromise of the general enterprise IT environment. Effective segmentation includes network-level separation, access restrictions, and connectivity restrictions.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

a) Overall design goals for implementing environment ~~segregation~~separation

- Implement a "secure zone" to separate and protect the local SWIFT infrastructure from the compromise of systems and services located outside of the secure zone.
- To the fullest extent possible, passwords and other authenticators that are usable inside the secure zone (especially for privileged accounts) are not stored or used in any form (hashed, encrypted, or plain text) in systems outside of the secure zone. This does not apply to encrypted back-up files. If the authentication services system resides outside of the SWIFT secure zone, then:
  - Either the system is in another existing secure zone that has similar controls,
  - or the system is only used to filter the connections to the SWIFT infrastructure component (controlling the connectivity at the boundary of the secure zone). In such a case, logical access to the SWIFT infrastructure component is ensured by another authentication mechanism residing in the secure zone (another IAM or the accessed component itself).
- The secure zone is appropriately scoped to each user's environment, including the potential reuse of existing secure zones (for example, a secure "production environment", "back-office environment", or "payment systems zone") to include the local SWIFT infrastructure.
- The components within the secure zone are all protected to the same or an equivalent level of security, access control, and trust and may communicate freely within the zone. Primary purpose of a secure zone is to host SWIFT-related components but can also include non-SWIFT related systems which then also need to be adequately protected by applying controls applicable to the SWIFT-related components (see the CSP FAQ for the relevant controls).
- Appendix B contains illustrative architecture diagrams that show samples of the methods a secure zone can be designed.

b) Scope of the secure zone

- The secure zone contains, but is not limited to, all components of the local SWIFT infrastructure. This includes the messaging interface, the communication interface, the browser-based GUI, the SWIFTNet Link, the Hardware Security Module (HSM), the SWIFT connector, the jump server (see details below), and any applicable operator PCs solely dedicated to the operation or administration of the local SWIFT infrastructure.
  - General-purpose operator PCs are not included in the secure zone.
  - Dedicated operator PCs with SWIFT-related software installed (that is, "thick client" GUI software) are located in the secure zone, or the software is installed only on the jump server to be accessed by the general-~~-~~purpose operator PCs outside of the secure zone.
  - Back-office and middleware systems (for example, IBM® MQ servers) used for data exchange with back-office systems are not necessarily included in the secure zone, but may be considered for inclusion depending on the chosen size and scope of the secure zone.
  - Test systems are not considered in scope of the security controls as long as (i) they are fully separated from production or live environment (including separate HSMs) and (ii) they are configured to only support test traffic (for example, by only using lite certificates on test-only logical terminals). If the test systems are not fully separated or can be configured for live traffic, then users must take the test systems in scope and make sure that the same security controls are applied as for production or live systems.~~Test systems are preferably fully segregated from production systems (including separate HSMs) and are configured to only support test traffic (for example, by only using lite certificates and only configuring test logical terminals). If not fully segregated, then these systems must be maintained to the same security level as the production systems.~~ Development systems are not within the secure zone and are not connected to the SWIFT network.
  - The Alliance Connect SRX VPN boxes or the Alliance Connect ~~v~~Virtual VPN instances (hosting systems or machines) are in a secure environment with appropriate physical controls (aligned with control 3.1).
- The secure zone size and scope are defined in a way that is most appropriate to the user's environment. Options may include, but are not limited to the following:
  - A SWIFT secure zone dedicated only for the local SWIFT infrastructure.
  - An expansion of an existing secure area (for example, a secure "production environment" or "payment systems zone") to include the local SWIFT infrastructure. The size and scope of this zone may vary significantly depending on the existing environment.
- Software, systems, and services within the secure zone are assessed for need and removed from the zone if not supporting the operations or security of the zone (for example, assess the need for e-mail access).

c) Protection of the secure zone

Boundary Protection

- Transport layer stateful firewalls are used to create logical separations at the boundary of the secure zone.
  - Transport layer firewalls creating the secure zone boundary should be physically or virtually dedicated to the protection of the secure zone. If a firewall is shared to separate other zones, then care must be taken for the firewall management to make sure that compromises of the firewall do not affect the protection of the secure zone.
  - Access control lists (ACLs) and application firewalls may be used to provide additional protection for the secure zone, but are not sufficient alone.
- Layer 2 devices (data link layer, such as switches) may be shared between the secure zone and other uses (VLAN ~~segregation~~separation).
- Administrative access to networking devices is protected using either an out-of-band network or through controlled in-band access (for example, a management VLAN). Administrative access to the firewalls that protect the secure zone does not rely on the enterprise user authentication system, but a system located within an existing secure zone that has similar controls as the SWIFT secure zone.
- Inbound and outbound connectivity for the secure zone is limited to the fullest extent possible. A process is implemented to analyse, review, and enforce the firewall rules governing the connectivity.
  - No "allow any" firewall rules are implemented, and network flows are explicitly authorised (allow listing approach). To achieve this, a general enterprise server might initially be used to filter legitimate connectivity access towards the secure zone without losing traceability of such connections.
  - Generally, connectivity crossing the secure zone boundary is restricted to bi-directional communications with back-office applications and MV-SIPN[16], inbound communications from approved general-purpose operator PCs to the jump server, and outbound administration data (data logging, back-ups).
  - Firewall rules are reviewed annually, at least.
  - Connections through the boundary firewalls are logged.

d) Access to the secure zone systems

d.1 Local Operator (end user and administrator) Access

- The secure zone has implemented one of the following designs for restricting operator access (interactive or command-line sessions) into the secure zone:
  - Operators connect from dedicated operator PCs located within the secure zone (that is, PCs located within the secure zone, and used only for secure zone purposes).
  - Operators connect from their general-purpose operator PC to the secure zone through a jump server (for example, using a Citrix-type solution or Microsoft Terminal Server) located within the SWIFT secure zone or within another existing secure zone that has similar controls.
    As the entry point into the secure zone, the jump server implements strong security practices, including the following:
    - Make sure all in-scope security controls in this document are implemented (for example security updates, system hardening).
    - Separate jump server for system administrators (with multi-factor authentication) and end users. As an alternative to separate jump servers, only allow temporary access to system administrators with effective approval processes and session activity recording.
    - Restrict access to authorised operators only.
    - Remove any unnecessary software.
    - Restrict risky activity (for example, sending or receiving e-mails).
    - Enable logging.
  - Operators connect from their general-purpose operator PC and only access the messaging or communication interface with a browser-based GUI (for example, Alliance Web Platform). The following specific security controls apply to this set-up:
    - The browser-based GUI is located in the secure zone and is logically separated from the messaging and communication interface.
    - Multi-factor authentication is implemented, where appropriate (on the browser-based GUI, on the messaging interface, or on the communication interface).

[16] Multi-Vendor Secure IP Network

- This set-up cannot be used for operating system administration activities.

- SWIFT systems within the secure zone restrict administrative access to only expected ports, protocols, and originating IPs.

d.2 Remote Operator Access (teleworking, "on-call" duties, or remote administration)

- Remote access to the secure zone from outside of the local user network first requires VPN authentication (recommended with multi-factor authentication) to the local network before accessing the secure zone through the same secured channels as local operators.
- A risk assessment is performed by the user to consider ~~additional~~ appropriate security controls to be implemented for remote access, such as the use of a virtual desktop infrastructure, dedicated channels for connectivity (for example, dedicated jump servers for remote users, leased lines).

e) ~~Segregation~~ Separation from General Enterprise IT Services

- To protect the secure zone from credential theft or a compromise of enterprise authentication (LDAP, RADIUS, Identity Provider, multi-factor) services, or a combination of both, secure zone systems use a separate authentication system from the general enterprise authentication service. For example, secure zone systems are not a member of the corporate directory service, but are instead members of a secure zone directory service.
- Supporting IT infrastructure, such as asset management, databases, data storage, security services (for example, patching), and networking services (for example, DNS, NTP) used within the secure zone is protected from credential compromise within the larger enterprise. Institutions must conduct an analysis of connectivity points which make sure that these systems do not store authenticators (passwords, tokens, and other methods) for systems and accounts in scope in any format (hashed, encrypted, plain text) outside of the secure zone or another existing secure zone that has similar controls. The supporting IT infrastructure should not be exclusive to SWIFT systems and may be shared within the secure zones.

Optional Enhancements:

- Systems within the secure zone implement (when technically possible) application allowlisting, which allows only trusted applications to be executed.
- Restrict (through additional separation) the communication between components of the secure zone considering the following:
  - Network ACLs or host-based firewalls that restrict traffic on a host-by-host basis within the secure zone.
  - Individual hardware or network-based firewalls between the components in the secure zone can optionally be used.

Considerations for alternative implementations:

Institutions with a high level of security programme maturity within the organisation might consider implementing alternative controls such as those suggested below or others. The alternative solutions must be risk-appropriate to each environment, and must consider the effort required to effectively implement, manage, and maintain the solution.

- Not separating secure zone authentication services from the enterprise authentication service will require implementing a comprehensive set of defence-in-depth controls to protect from and detect adversaries that cross the secure zone boundary. Controls may include locating the authentication service within an existing secure zone with similar controls as those applicable to the SWIFT secure zone, limiting trust relationships between the larger enterprise environment and the secure zone (such as one-way trust relationships), restricting operator and administrative access, implementing strong privileged access controls, implementing read-only access where feasible, enabling verbose logging, and implementing centralised active monitoring and detective capabilities.
- If general enterprise IT services (for example, vulnerability scanning and boundary firewall management) are shared between the secure zone and other environments, then any credentials used across the environment should be monitored to make sure they are only used when and where expected.
- If a general enterprise server is initially used to reach the secure zone, then that server is only used to filter legitimate connectivity access (as a concentrator or gateway to ease access filtering to the secure zone). Identity and access management for secure zone components or the jump server (or both) still rely on authentication services that reside within the SWIFT secure zone or another existing secure zone that has similar controls.

- If the secure zone has dependencies on enterprise shared functions (such as directory services, servers, or networks) that are outside the scope, then the user must make sure that any compromise of such functions will not compromise the security of the in-scope components.

1.2 Operating System Privileged Account Control

Control Type: Mandatory / Advisory for B	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Restrict and control the allocation and usage of administrator-level operating system accounts.

In-scope components:

Administrator-level accounts defined on the following components:

- ~~Secure zone: administrator-level operating system accounts (on physical~~ systems or virtual machines (VMs) hosting a SWIFT-related component (including interface, GUI, SWIFT or customer connector)
- dedicated operator PCs
- network devices protecting the secure zone~~)~~
- Local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) that hosts SWIFT-related VMs~~: platform administrator-level accounts~~
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) u~~ti~~lised for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~•~~
- ~~[Advisory A4: Customer connector]~~[Advisory: General-purpose operator PCs]

Risk Drivers:

- deletion of logs and forensic evidence
- excess privilege or access
- lack of traceability
- unauthorised system changes

Implementation Guidance

Control Statement:

Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used.

Control Context:

Tightly protecting administrator-level accounts within the operating system reduces the opportunity for an attacker to use the privileges of the account as part of an attack (for example, executing commands or deleting evidence).

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Examples of a~~A~~dministrator-level accounts are defined as follows:
  - Windows: built-in administrator account and members of groups with administrator privileges (for example, accounts with debug or file system privileges). Typically, Enterprise Admins group, Domain Admins group, and Local Administrator group.

- Linux/Unix: root account (User ID = 0) and members of the root group.
- Mainframe: system administrator or system programmer role.
- Network devices: accounts like admin, root, telco, su or cisco.

- Access to administrator-level operating system accounts is restricted to the maximum extent possible unless needed to install, configure, maintain, operate, or support emergency activities. The use of the administrator-level account is limited to the duration of the activity (for example, maintenance windows).
- Logins with built-in administrator-level accounts are not permitted, except to perform activities where such accounts are specifically needed (for example, system configuration) or in emergency situations (break-glass account). Individual accounts with administrator-level privileges or accounts with the ability to escalate to administrative access, (like "sudo") are used instead.
- Individual administrator-level account access and usage are logged so that activities can be reconstructed to determine the root-cause of incidents.
- Administrator-level passwords are tightly controlled with physical access controls when physically recorded.

Optional Enhancements:

- Systems are configured to not allow logins of built-in administrator-level accounts, except through a maintenance mode (for example, single user mode or safe mode). This effectively prohibits logins to the account as a service, batch job, through remote desktop services, or by escalating privileges from another account.

Considerations for alternative implementations:

New models are emerging to enhance the user experience but also availability as observed with the pandemic. Alternative implementations are raising to give users flexible access to the institutions' environment: not necessarily through fully managed devices[17] but incorporating also individuals own devices to reach resources located on premises or in the cloud. That implies moving from a controlled on-premises environment (for which the CSCF mainly provides guidance) to a zero-trust environment requiring to assess and control appropriately each type of access.

Such alternatives have to be considered individually and specifically by users from a risk-based point of view taking into consideration potential risks if some elements are compromised. Those alternatives cannot be described here but would require to consider elements such as those identified below for a secure virtual desktop infrastructure:

- Defining a virtual desktop infrastructure (Citrix or other workspace) with OS privileged account managed centrally and not possibly activated or used by the end users can meet the control (considering the virtual infrastructure is protected in line with control 1.3 and the virtual desktops themselves are protected as a physical general-purpose operator PC in line with control such as 2.2, 2.3, 2.7, 4.1, 5.1; 6.1; 6.4, 6.5A).
- The risks of end-user device compromise must be considered, analysed and appropriate controls deployed to protect the virtual desktop infrastructure and further accessed resources. Those controls must ensure proper authentication, activities authorisation (requesting sometimes additional independent factors) but also appropriate prompt reaction, involving also the end users, in case of end-user device compromise, loss or theft to block potential accesses through such device.
- Confidentiality and integrity of the sessions established towards the virtual infrastructure must also be ensured in line with the standard operator session depicted in control 2.6.

[17] Fully managed device is a company-owned device with features that give IT admins control of the device settings and policy configuration. At the opposite of the spectrum, there is usage of unmanaged (by a company) individuals own device to access the company resources, network or applications hosted in the cloud or by a service provider. Intermediary models can exist where managed (sand-boxed) application(s) (by a company) are deployed on users own device. All those models have to be properly analysed for proper and secure usage.

1.3 Virtualisation Platform Protection

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	

Control Definition

Control Objective: Secure the virtualisation platform and virtual machines (VMs) that host SWIFT-related components to the same level as physical systems.

In-scope components:

- Local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) and VMs used to host any of the following SWIFT-related components:
  - messaging interface
  - communication interface
  - GUI
  - SWIFTNet Link
  - SWIFT and customer connector
  - jump server
  - dedicated and general-purpose operator PCs
  - firewalls
  - [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) utilised to for data exchange between back-office and with SWIFT-related components]
  - [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
  - ~~[Advisory A4: Customer connector]~~
  - Alliance Connect Virtual VPN instance

***Note**: This requirement is not applicable when there is no local and remote virtualisation platform and no VMs used to host the referred SWIFT-related components.*

Risk Drivers:

- unauthorised access
- uncontrolled proliferation of systems and data

Implementation Guidance

Control Statement:

Secure the virtualisation platform, virtualised machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems.

Control Context:

Security controls that apply to non-virtualised (physical) systems are equally applicable to virtual systems. The additional virtualisation layer needs extra attention from a security perspective. The uncontrolled proliferation of VMs could lead to unaccounted machines with the risk of unmanaged, unpatched systems open to unauthorised access to data.

If appropriate controls have been implemented to this underlying layer, then SWIFT does not limit the use of virtual technology for any component of the local SWIFT infrastructure or the associated supporting infrastructure (for example, virtual firewalls).

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be

considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

When relying on a third party for the underlying virtualisation platform, the user must engage with the third party to obtain reasonable comfort that the control objective is met.

- The same security requirements apply to the virtualisation platform, virtual machines, and supporting virtual infrastructure as for all other infrastructure systems and components. Those security requirements cover, for example, the location in an existing secure zone that has similar controls as those applicable to the SWIFT or customer secure zone, privileged access restrictions, login and password policies, installation of security updates, and restriction of internet access. Those controls have the virtualisation platform identified in the *In-scope Components* section.
- Vulnerability scanning is performed on SWIFT-related VMs and, when technically possible, on the virtualisation platform.
- The virtualisation platform hosts are subject to physical protection, which prevents unauthorised physical access.
- VM isolation is ensured on the virtualisation platform to prevent the lateral move out of a virtual machine to access or interact with other VMs (or the underlying hypervisor) or to bypass normal network controls that filter or inspect connections to the SWIFT environment (or a combination of both).
    - Filtering and expected inspections of the network flows that reach the SWIFT-related VMs are performed preferably using resources (such as firewalls, packet inspections, or content filtering) external to the virtualisation platform or must be enforced at the hypervisor level.
    - If isolation is ensured on the virtualisation platform, then the hosted VMs can maintain their security classification and can be individually secured accordingly (as such, they do not inherit the classification of the SWIFT-related VMs and are not subject to all SWIFT-related controls).
- When multi-factor authentication is implemented for interactive access to the SWIFT-related VM operating systems (and in-line with control 4.2) to also prevent direct access to those VMs from the hypervisor layer, then multi-factor authentication is not mandatory at the virtualisation platform management level.

1.4 Restriction of Internet Access

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Control/Protect Internet access from operator PCs and systems within the secure zone.

In-scope components:

- dedicated and general-purpose operator PCs
- jump server
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) used for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~
- [Advisory: Local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) and their management PCs]
- messaging interface
- communication interface
- GUI
- SWIFTNet Link
- SWIFT and customer connector

Risk Drivers:

- exposure to internet-based attacks

Implementation Guidance

Control Statement:

All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business[18].

Control Context:

Direct access to the Internet raises exposure to internet-based attacks. Risk is even higher in case of human interactions (browsing, e-mails, or other social network activities being permitted). Once compromised, those systems can be an entry point that allows lateral movements or injection of command and control elements (or a combination of both).

If reducing the attack surface and vulnerabilities of those systems (as per the relevant controls identified in this document) is primordial, then limiting and controlling direct Internet accesses is crucial.

On top of (general) operator PCs that connect SWIFT-related services or applications offered by service providers (such as SWIFT in the case of Alliance Lite2 or Alliance Cloud, a Service Bureau, or an L2BA provider), due diligence must be taken to secure (general) operator PCs used to access local interfaces or GUIs. Insecurely combining access to the "production environment" and the Internet could be abused by attackers.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are

[18] Purpose is not to prohibit internet access but to limit/control connectivity where it is relevant for business related reasons (such as to access external service provider resources).

not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

a) Internet access from the secure zone

- General-purpose internet browsing (including e-mail activities) from systems within the SWIFT or customer secure zone is not permitted.
- Internet access from systems within the secure zone (for example, dedicated operator PCs or other SWIFT-related components) is highly restricted and ideally should be blocked.
  - When possible, activities that require the Internet are conducted outside of the secure zone. Example activities may include conducting daily business on swift.com, or downloading security updates for secure transfer into the secure zone.
  - If internet access is needed from within the secure zone, then access should be granted only to allow listed URL destinations through a proxy with content inspection and adequate blocking or filtering controls. Connections are only permissible if they are initiated in the outbound direction.
- As the entry point into the secure zone, the jump server (located within the secure zone or another existing secure zone that has similar controls) does not have internet access.

b) Internet access from general-purpose operator PCs

- Control internet access provided on the general-purpose operator PCs used with the following purposes:
  - Connect to an application at the service provider (user-to-application) to process financial transactions[19].
  - Access a messaging or communication interface through a browser-based GUI (for example, Alliance Web Platform).

  Control access through one of the following options:
    - internet access through a remote desktop or virtual machine solution
    - internet access from the general-purpose operator PC to only allow listed URL destinations through a proxy with content inspection, in combination with adequate blocking or filtering controls and permitting only outbound initiated connections
    - internet access from the general-purpose operator PC through a Web Gateway (with content inspection, in combination with blocking or filtering controls) using maintained denylisted URL destinations
- Even if SWIFT strongly recommends controlling the internet access, another method to meet the control objective on those PCs accessing the local SWIFT infrastructure is to enforce the usage of a jump server that has no internet access combined with multi-factor authentication (in line with control 4.2) implemented on the individual SWIFT-related ~~applications~~components/systems or at the jump server.

c) Internet access from other components (middleware servers or the virtualisation platform - Advisory)

- When used, internet access from the middleware system (such as an IBM® MQ server) or the virtualisation platform underlying system (also referred to as the hypervisor) is highly restricted and ideally blocked.
  - When possible, activities that require the Internet are conducted from other systems. Examples of such activities include conducting daily business, or downloading security updates for secure transfer into the target system.
- If internet access is needed from those systems, then access should be granted only to allow listed URL destinations through a proxy with content inspection and adequate blocking or filtering controls. Connections are only permissible if they are initiated in the outbound direction.

[19] Such as ~~posting~~, creating, submitting, approving or modifying messaging transactions or updating entitlements. Read-only/queries kind of access can be waived if entitlements cannot be changed from such operator PC's.

1.5A Customer Environment Protection

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		○	○	○	●	

Control Definition

Control Objective: Ensure the protection of the customer's connectivity infrastructure from external environment and potentially compromised elements of the general IT environment.

In-scope components:

- Customer connector
- dedicated and general-purpose operator PCs
- jump server

***Note**:* This control must be considered by Architecture types A1, A2 and A3 when a customer connector is also present outside of an existing SWIFT secure zone.

Risk Drivers:

- compromise of enterprise authentication system
- compromise of user credentials
- credential replay
- exposure to internet-based attacks
- unauthorised access

Implementation Guidance

***Note**:* This is almost a copy of control 1.1 focusing on the customer connector and expected usual separation between operational (or production) environment and the wider or general IT environment.

Control Statement:

A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment.

Control Context:

Segmentation between the customer's connectivity infrastructure and its larger enterprise network reduces the attack surface and has shown to be an effective way to defend against cyber attacks that commonly involve compromise of the general enterprise IT environment. Effective segmentation will include network-level separation, access restrictions, and connectivity restrictions.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

a) Overall design goals for implementing environment separation

- Implement a secure zone (or restricted operational zone) to separate and protect the customer connectivity infrastructure from the compromise of systems and services located outside of the secure zone.
- To the fullest extent possible, passwords and other authenticators that are usable inside the secure zone (especially for privileged accounts) are not stored or used in systems outside of the secure zone. This does not apply to encrypted back-up files.

- If the authentication services system resides outside of the secure zone, then:
  - Either the system is in another existing secure zone that has similar controls,
  - or the system is only used to filter the connections to the customer's connectivity infrastructure (controlling the accesses at the boundary of the secure zone). In such a case, logical access to the component is ensured by another authentication mechanism residing in the secure zone (by another IAM or is performed by the accessed component itself).
- The secure zone is appropriately scoped to each user's environment, including the potential reuse of existing secure zones (for example, a secure "production environment", "back-office environment", or "payment systems zone") to include the connectivity infrastructure.
- The components within the secure zone are all protected to the same or an equivalent level of security and trust and those components may communicate freely within the zone. Primary purpose of a secure zone is to host SWIFT-related components but can also include non-SWIFT related systems which then also need to be adequately protected by applying controls applicable to the SWIFT-related components (see the CSP FAQ for the relevant controls).

b) Scope of the secure zone

- The secure zone contains, but is not limited to, all components of the connectivity infrastructure. This includes the Hardware Security Module (when relevant), the customer connector, the jump server (see details below), and any applicable operator PCs solely dedicated to the operation or administration of the connectivity infrastructure. As such:
  - General-purpose operator PCs are not included in the secure zone.
  - Dedicated operator PCs with "thick client" GUI software are located in the secure zone, or the software is installed on the jump server and accessed by the general- purpose operator PCs residing outside of the secure zone.
  - Back-office systems are not necessarily included in the secure zone, but may be considered for inclusion depending on the chosen size and scope of the secure zone.
  - Test systems are not considered in scope of the security controls as long as (i) they are fully separated from production or live environment (including separate HSMs, when used) and (ii) they are configured to only support test traffic (for example, by only using lite certificates on test only logical terminals). If the test systems are not fully separated or can be configured for live traffic, then users must take the test systems in scope and make sure that the same security controls are applied as for production or live systems. Development systems are not within the secure zone and are not connected to the SWIFT network.
  - When used, the Alliance Connect SRX VPN boxes or the Alliance Connect Virtual VPN instances (hosting systems or machines) are in a secure environment with appropriate physical controls (aligned with control 3.1).
- The secure zone size and scope are defined in a way that is most appropriate to the user's environment. Options may include, but are not limited to the following:
  - A specific secure zone dedicated only for the connectivity infrastructure.
  - An expansion of an existing secure area (for example, a secure "production environment" or "payment systems zone") to include the connectivity infrastructure. The size and scope of this zone may vary significantly depending on the existing environment.
- Software, systems, and services within the secure zone are assessed for need and removed from the zone if not supporting the operations or security of the zone (for example, assess the need for e-mail access).

c) Protection of the secure zone

Boundary Protection

- Transport layer stateful firewalls are used to create logical separations at the boundary of the secure zone.
  - Transport layer firewalls creating the secure zone boundary should be physically or virtually dedicated to the protection of the secure zone. If a firewall is shared to separate other zones, then care must be taken for the firewall management to make sure that compromises of the firewall do not affect the protection of the secure zone.
  - Access control lists (ACLs) and application firewalls may be used to provide additional protection for the secure zone, but are not sufficient alone.

- Layer 2 devices (data link layer, such as switches) may be shared between the secure zone and other uses (VLAN separation).
- Administrative access to networking devices is protected using either an out-of-band network or through controlled in-band access (for example, a management VLAN). Administrative access to the firewalls that protect the secure zone does not rely on the enterprise user authentication system, but a system located within an existing secure zone that has similar controls.
- Inbound and outbound connectivity for the secure zone is limited to the fullest extent possible. A process is implemented to analyse, review, and enforce the firewall rules governing the connectivity.
  - No "allow any" firewall rules are implemented, and network flows are explicitly authorised (allow listing approach). To achieve this, a general enterprise server might initially be used to filter legitimate connectivity access towards the secure zone without losing traceability of such connections.
  - Generally, connectivity crossing the secure zone boundary is restricted to bi-directional communications with back-office applications and MV-SIPN[20], inbound communications from approved general-purpose operator PCs to the jump server, and outbound administration data (data logging, back-ups).
  - Firewall rules are reviewed annually, at least.
  - Connections through the boundary firewalls are logged.

d) Access to the secure zone systems

d.1 Local Operator (end user and administrator) Access

- The secure zone has implemented one of the following designs for restricting operator access (interactive or command-line sessions) into the secure zone:
  - Operators connect from dedicated operator PCs located within the secure zone (that is, PCs located within the secure zone, and used only for secure zone purposes).
  - Operators connect from their general-purpose operator PC to the secure zone through a jump server (for example, using a Citrix-type solution or Microsoft Terminal Server) located within the secure zone or within another existing secure zone that has similar controls.
    As the entry point into the secure zone, the jump server implements strong security practices, including the following:
    - Make sure all in-scope security controls in this document are implemented (for example security updates, system hardening).
    - Separate jump server for system administrators (with multi-factor authentication) and end users. As an alternative to separate jump servers, only allow temporary access to system administrators with effective approval processes and session activity recording.
    - Restrict access to authorised operators only.
    - Remove any unnecessary software.
    - Restrict risky activity (for example, sending or receiving e-mails).
    - Enable logging.
  - Operators connect from their general-purpose operator PC and only access the customer connector offering interactive access with a browser-based GUI. The following specific security controls apply to this set-up:
    - The browser-based GUI is located in the secure zone and is ideally logically separated from the customer connector.
    - Multi-factor authentication is implemented, where appropriate (on the browser-based GUI or on the customer connector).
    - This set-up cannot be used for operating system administrative activities.
- Customer connectivity systems within the secure zone restrict administrative access to only expected ports, protocols, and originating IPs.

d.2 Remote Operator Access (teleworking, "on-call" duties, or remote administration)

- Remote access to the secure zone from outside of the user network first requires VPN authentication (recommended with multi-factor authentication) to the network before accessing the secure zone through the same secured channels as local operators.
- A risk assessment is performed by the user to consider additional security controls to be implemented for remote access, such as the use of a virtual desktop infrastructure, dedicated channels for connectivity (for example, dedicated jump servers for remote users, leased lines).

[20] Multi-Vendor Secure IP Network

e) Separation from General Enterprise IT Services

- To protect the secure zone from credential theft or a compromise of enterprise authentication (LDAP, RADIUS, Identity Provider, multi-factor) services, or a combination of both, secure zone systems use a separate authentication system from the general enterprise authentication service. For example, secure zone systems are not a member of the corporate directory service, but are instead members of a secure zone directory service.
- Supporting IT infrastructure, such as asset management, databases, data storage, security services (for example, patching), and networking services (for example, DNS, NTP) used within the secure zone is protected from credential compromise within the larger enterprise. Institutions must conduct an analysis of connectivity points which make sure that these systems do not store authenticators (passwords, tokens, and other methods) for systems and accounts in scope in any format (hashed, encrypted, plain text) outside of the secure zone or another existing secure zone that has similar controls. The supporting IT infrastructure should not be exclusive to SWIFT systems and may be shared within the secure zones.

Optional Enhancements:

- Systems within the secure zone implement (when technically possible) application allow listing, which allows only trusted applications to be executed.
- Restrict (through additional separation) the communication between components of the secure zone considering the following:
  - Network ACLs or host-based firewalls that restrict traffic on a host-by-host basis within the secure zone.
- Individual hardware or network-based firewalls between the components in the secure zone can optionally be used.

Note: SWIFT expects this control to become mandatory in the next version of this document.

Considerations for alternative implementations:

Institutions with a high level of security programme maturity within the organisation might consider implementing alternative controls such as those suggested below or others. The alternative solutions must be risk-appropriate to each environment, and must consider the effort required to effectively implement, manage, and maintain the solution.

- Not separating secure zone authentication services from the enterprise authentication service will require implementing a comprehensive set of defence-in-depth controls to protect from and detect adversaries that cross the secure zone boundary. Controls may include locating the authentication service within an existing secure zone with similar controls as those applicable to the secure zone, limiting trust relationships between the larger enterprise environment and the secure zone (such as one-way trust relationships), restricting operator and administrative access, implementing strong privileged access controls, implementing read-only access where feasible, enabling verbose logging, and implementing centralised active monitoring and detective capabilities.
- If general enterprise IT services (for example, vulnerability scanning and boundary firewall management) are shared between the secure zone and other environments, then any credentials used across the environment should be monitored to make sure they are only used when and where expected.
- If a general enterprise server is initially used to reach the secure zone, then that server is only used to filter legitimate connectivity access (as a concentrator or gateway to ease access filtering to the secure zone). Identity and access management for secure zone components or the jump server (or both) still rely on authentication services that reside within the secure zone or another existing secure zone that has similar controls.
- If the secure zone has dependencies on enterprise shared functions (such as directory services, servers, or networks) that are outside the scope, then the user must make sure that any compromise of such functions will not compromise the security of the in-scope components.

2 Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•		

Control Definition

Control Objective: Ensure the confidentiality, integrity, and authenticity of application data flows between local SWIFT-related components~~applications~~.

In-scope components:

- ~~jump server (when used)~~
- local or remote (hosted and or operated by a third party, or both) SWIFT~~-related~~ infrastructure and related components

Risk Drivers:

- loss of sensitive data confidentiality
- loss of sensitive data integrity
- unauthenticated system traffic
- unauthorised access
- password theft

Implementation Guidance

Control Statement:

Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT-related ~~application~~component-to-~~application~~ component or system-to-system data flows ~~and, when used, jump server-to-application data flows~~.

Control Context:

The protection of internal data flows safeguards against unintended disclosure, modification, and access of the data while in transit.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- All data flows between SWIFT-related components~~applications~~ are protected using a secure mechanism (for example, by using Local Authentication (LAU) in combination with a confidentiality protection[21] or by using two-way TLS) to support the confidentiality, integrity, and mutual authentication of the data flows. This includes the following data flows:
  - RMA application to messaging interface
  - GUI to messaging interface
  - GUI to communication interface
  - messaging interface to communication interface

[21] Such as one-way TLS

- ~~The communication between the jump server (when used) and the SWIFT-related applications is protected using a secure mechanism (for example, one-way TLS) to support the confidentiality and integrity of the user's connection to the applications.~~
- Secure protocols use current, commonly accepted cryptographic algorithms (for example, AES[22] and ECDHE[23]) with key lengths in line with the current best practices. For more information about cryptographic algorithms that support secure protocols, see SWIFT Knowledge Base article 5021566.
- Credentials and private keys used, and usually stored, by the applications to secure the flows are protected (large spectrum of protection, from definition and usage of secure coding guidelines to usage of specific solutions, can be envisaged based on user's risk management).

[22] Advanced Encryption Standard
[23] Elliptic Curve Diffie-Hellman Ephemeral

2.2 Security Updates

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Minimise the occurrence of known technical vulnerabilities on operator PCs and within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.

In-scope components:

Hardware and software of the following components:

- physical systems or virtual machines (VMs) hosting a SWIFT-related component (including interface, GUI, SWIFT or customer connector)
- dedicated and general-purpose operator PC ~~and, when used, jump server (all hardware and software)~~
- jump server
- local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs and their management PCs
- ~~secure zone: all hardware including~~ network devices protecting the secure zone~~and software~~
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) u~~ti~~sed for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~

Risk Drivers:

- exploitation of known security vulnerabilities

Implementation Guidance

Control Statement:

All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.

Control Context:

The closure of known security vulnerabilities is effective in reducing the various pathways that an attacker may use during an attack. A security update process that is comprehensive, repeatable, and implemented in a timely manner is necessary to continuously close these known vulnerabilities when security updates are available.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Vendor support
  - All software (including operating systems) and hardware (including network devices) are within the actively supported product life-cycle window of the vendor (including extended support), if applicable.
  - Maintenance or licensing contracts are in place for access to updates, minor upgrades, and other critical maintenance functions.
- Mandatory software updates

- Mandatory releases or updates that are applicable to a local SWIFT component are installed within the deadline specified by the vendor.

- Application of security updates
  - A risk assessment process is in place to determine the most appropriate treatment of vendor security updates. Risk assessment considerations may include the vendor-reported criticality of the update, user exposure and vulnerability, mitigating controls, and operational impact.
  - User-defined deployment timelines are established for applying updates based on criticality, system type, and required update testing.
  - In the absence of established internal processes and timelines, SWIFT recommends the use of the Common Vulnerability Scoring System (CVSS) Version 3 as a guideline for criticality, with the following update deployment targets:
    - Critical (9.0+ score): applied within one month of release
    - High (7.0 - 8.9 score): applied within two months of release
    - Low / Medium (< 7.0 score): user defined

    Note: It is common practice that operating system security updates are automatically pushed and applied on the Operator PCs shortly after their publication by the provider.

- Source and integrity validation of software and security updates.

- Before applying the software and security updates, the legitimate source is validated and integrity checks (for example, checksum validation) are performed when technically possible.

2.3 System Hardening

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Reduce the cyber-attack surface of SWIFT-related components by performing system hardening.

In-scope components:

- ~~operating systems for~~ dedicated and general-purpose operator PC
- ~~and~~ jump server ~~(when used)~~
- ~~operating systems for~~ systems (physical or VMs) hosting a SWIFT-related component (including interface, GUI, SWIFT and customer connectors) ~~SWIFT-related applications (including VMs)~~
- local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs and their management PCs
- network devices protecting ~~supporting infrastructure within~~ the secure zone ~~(for example, firewalls or routers)~~
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) u~~til~~ised for data ~~to~~ exchange between back-office and ~~with~~ SWIFT-related components]
- ~~[Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]~~
- ~~[Advisory A4: Customer connector]~~

Note: SWIFT HSMs are FIPS 140-2 Level 3 compliant with hardened underlying OS and are out of the scope of this control.

Risk Drivers:

- excess attack surface
- exploitation of insecure system configuration

Implementation Guidance

Control Statement:

Security hardening is conducted and maintained on all in-scope components.

Control Context:

System hardening applies the security concept of "least privilege" to a system by disabling features and services that are not required for normal system operations. This process reduces the system capabilities, features, and protocols that a malicious person may use during an attack.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- All in-scope systems are hardened, considering one or more of the following:
  - vendor security configuration guidance

- industry-standard security configuration guidance (for example,[24] 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

- The selected hardening configuration (set of rules) can be overruled by application-specific configuration requirements to maintain a proper operational state for SWIFT-related systems.
- At a minimum, the hardening process should do the following:
  - Change default passwords.
  - Disable or remove unnecessary user accounts.
  - Disable or restrict unnecessary services, ports, and protocols.
  - Remove unnecessary software.
  - Restrict physical ports (for example, USBs) as appropriate.
  - Set, when technically possible, auto-lock options (such as activating an operator PC screen saver requiring a login after an inactivity time-out or when turned to sleep mode). A 15-minute inactivity time-out is recommended.
  - Adjust any default configurations known to be vulnerable.

  The vendor and industry standards listed above can provide detailed guidance to accomplish these minimum targets.
- Deviations from the selected hardening configuration are documented along with justification for the deviation and potential mitigations applied.
- Systems are maintained secure, as follows:
  - by checking regularly (at least twice per year) the systems against the secure settings identified as per preceding guidance to take any relevant corrective actions
  - by regularly applying the identified secure settings to the systems.

[24] Center for Internet Security; Defense Information Systems Agency - Secure Technical Implementation Guide; National Institute of Standards and Technology

2.4A Back Office Data Flow Security

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure the confidentiality, integrity, and mutual authenticity of data flows between local or remote SWIFT infrastructure components and the back-office first hops they connect to.

In-scope components:

- Data exchange layer: flows of financial transactions between the local or remote (hosted or operated by a third party, or both) SWIFT-related components (interfaces, GUI or SWIFT and customer connectors) and the back-office first hops at the application level they are connected to (directly or through middleware).

Risk Drivers:

- loss of sensitive data confidentiality
- loss of sensitive data integrity
- unauthenticated system traffic

Implementation Guidance

Control Statement:

Confidentiality, integrity, and authentication mechanisms (at system, transport~~mutual~~ or message level) ~~based authentication mechanisms~~ are implemented to protect data flows between SWIFT infrastructure components and the back-office first hops they connect to.

Control Context:

Protection of data flows or connections between the back-office first hops (at the application level) as seen from the SWIFT or customer secure zone and the SWIFT infrastructure safeguards against person-in-the-middle attack, unintended disclosure, modification, and data access while in transit.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Data flowing between local or remote (hosted or operated by a third party, or both) SWIFT-related components (such as interfaces or connectors) and the back-office systems (or middleware systems) they are directly connected to, is protected using a secure mechanism (for example, LAU in combination with a confidentiality protection, or another message-based authentication solution, XML DSIG, AES GCM Authenticated Encryption, or two-way TLS) that provides confidentiality, integrity, and mutual authentication of the data in transit. This includes the data flow between the following:
  - messaging interface and the first back-office (or middleware) hops as seen from the interface
  - communication interface and the first back-office (or middleware) hops as seen from the interface
  - connector and first back-office (or middleware) hops as seen from the connector
- Secure protocols use current, commonly accepted cryptographic algorithms (for example, AES[25] or ECDHE[26]) with key lengths in line with the current best practices. For more information about cryptographic algorithms that support secure protocols, see SWIFT Knowledge Base article 5021566.

[25] Advanced Encryption Standard
[26] Elliptic Curve Diffie-Hellman Ephemeral

- As this control is expected to become Mandatory gradually in a future release, the following guidelines are already provided to progressively reach compliance:
  - Possess an inventory of data flows between SWIFT-related components and the first back-office (or middleware) hops.
  - Possess a plan to implement/activate secure mechanisms for identified flows, considering the following:
    - Implement secure mechanisms (see the first guideline above) as exposed by the interfaces, connectors, or middleware server.
    - Migrate opportunistically legacy and less standard flows to secure mechanisms or protocols.
    - Mitigate (in the interim) the risk of back-office host spoofing or message injections through systems or network connectivity means.
- When a middleware server ~~or a customer connector~~ is used for data exchange with the back-office systems, some requirements are expected on the middleware server supporting hosts. Those hosts are the wardens of the data exchanged~~connections~~ between the back office and the SWIFT-related components ~~or SWIFT~~, as follows:
  - Irrespective of where the middleware server ~~or customer connector~~ hosts are located and shared with, the same security requirements apply to those hosts, such as channelled MQ servers used to reach a back-office first hop, as for other SWIFT-related components or infrastructure systems. Those security requirements cover the location in another secure zone that has similar controls as those applying to the SWIFT or customer secure zone, privileged access restrictions, login and password policy, installation of security updates, and restriction of internet access. Those controls have the middleware server ~~or the customer connector (or both)~~ identified as Advisory in the "In-scope components" of the control definition.
  - Protection of the data on the middleware servers (such as data present in the queues of MQ servers used to reach the back-office first hops) ~~or on the customer connector~~ must be ensured to prevent unauthorised access. This can be done by implementing thorough access controls or by encrypting queues or data at rest.
  - Protection of the SWIFT-related data that flows between the middleware server hosts (such as between several channelled MQ servers) should be safeguarded as part of the middleware infrastructure protection by using secure mechanisms (see the first item of the implementation guidelines above).
  - Definition and management of the connectivity rules and business flows on the middleware servers must be secured to prevent unauthorised flows.
- For middleware servers (such as IBM® MQ) that directly connect SWIFT infrastructure components, it is advised to also implement the same level of protection on the flows between this middleware server and the back-office first hops as seen from an application perspective by the SWIFT-related component. ~~Similarly, it is also advised to implement the same level of protection between a customer connector and the back-office first hops (if any) as seen from an application perspective.~~ To gradually reach control compliance for those links, the following guidelines are provided:
  - Possess an inventory of SWIFT-related data flows between the middleware server and the back-office first hops as seen from SWIFT-related component ~~and between a customer connector and the back-office first hops as seen from the customer connector~~.
  - Possess a plan to activate secure mechanisms for identified flows, considering the following:
    - Implement secure mechanisms (see the first item of the implementation guidelines above) as exposed by the middleware server ~~, the customer connector,~~ or the back-office system.
    - Migrate opportunistically legacy and less standard flows to secure mechanisms or protocols.
    - Safeguard (in the interim) the authentication of the data sources and authorisation of the SWIFT-related data through native middleware functionalities or through systems or network connectivity means that prevent host spoofing.
- Credentials and private keys used, and usually stored, by the applications to secure the flows are protected (large spectrum of protection, from proper coding guidelines to usage of specific solutions, can be envisaged based on user's risk management).

***Note**:* SWIFT expects this control to become Mandatory in a future version of this document and will phase the following expectations:

- ~~customer connector and~~ middleware servers (to start, when used)
- flows between the middleware servers and the SWIFT-related components
- SWIFT-related flows towards the back-office systems reached by the SWIFT-related components ~~or the customer connector,~~ directly or through the middleware server (to finish)

2.5A External Transmission Data Protection

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	

Control Definition

Control Objective: Protect the confidentiality of SWIFT-related data transmitted or stored outside of the secure zone as part of operational processes.

In-scope components:

- SWIFT-related secure zone sensitive data (such as back-ups, business transaction details, and credentials)

Risk Drivers:

- compromise of trusted back-up data
- loss of sensitive data confidentiality

Implementation Guidance

Control Statement:

Sensitive SWIFT-related data that leaves the secure zone as a result of operating system/application back-ups, business transaction data replication for archiving or recovery purposes, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit.

Control Context:

While **2.4A** covers the back-office application flows with the SWIFT-related components, this control covers the underlying SWIFT-related data that resides in the cloud or is exported from the secure zone and manipulated as per operational activities (such as back-ups or manual/automated data extraction/copies).

Operating system or applications back-ups and the replication of business transaction data can provide useful information to prepare fraudulent transactions. The transfer, handling, and storage outside of secure zones (when, for example, using the SAN/NAS[27] technology) must therefore be secured to prevent unauthorised access. Flow or data encryption are usual means to protect such data in transit.

Back-up encryption, encryption of data at rest, or appropriate authorisation and access controls are usual means to protect stored data.

Offline processing covers, for example, processing performed for support activities, additional analysis, or business intelligence activities.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Replicated or extracted SWIFT-related sensitive data (business transaction data that reveals details such as involved debtors, creditors, accounts, amounts, trade information), passwords, and other authenticators are as follows:
  - Protected from unauthorised access when stored outside of the SWIFT or customer secure zone or another secure zone that has similar controls as the SWIFT or customer secure zone. Such replicated or extracted data is also ideally encrypted when stored outside of a secure zone (this can be achieved either at the data, file, application, or system level).

[27] Storage Area Network / Network Attached Storage both providing network storage solutions

  - Encrypted when in transit between secure zones (for example, between data centres) or transferred outside of a secure zone (SWIFT or another zone that has similar controls). Encryption can be applied on the data or at the network/communication/transport layer.
- When relying on a remote virtualisation platform (hosted or operated by a third party, or both) it is recommended to ensure the encryption of the data. This can be obtained at the subscription level or at the storage level, expected to be offered by the third party to provide a guarantee in regard to access to stored data.
- Encryption protocols or mechanisms use a current, commonly accepted cryptographic algorithm (for example, AES[28] or ECDHE[29]) with key lengths in line with current best practices. For more information about cryptographic algorithms that currently support secure protocols, see SWIFT Knowledge Base article 5021566.
- Encryption mechanisms comply with applicable laws and regulations[30].
- If the cryptography protecting SWIFT-related sensitive data has been compromised, then a process should be established to apply new cryptography and secure or destroy any compromised copies of the data.

***Note*:** It is expected that back-ups kept for business or system recovery are maintained in a secure zone that has similar controls to the SWIFT or customer secure zone.

[28] Advanced Encryption Standard
[29] Elliptic Curve Diffie-Hellman Ephemeral
[30] Such as those identified by Global Partner Digital (https://www.gp-digital.org/world-map-of-encryption/)

2.6 Operator Session Confidentiality and Integrity

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Protect the confidentiality and integrity of interactive operator sessions that connect to the local or remote (operated by a service provider) SWIFT ~~-related~~ infrastructure or service provider SWIFT-related applications.

In-scope components:

Interactive user, operator or management sessions performed from

- dedicated and general-purpose operator PC
- jump server
- Any another intermediate host accessed or used from any of the above

to connect to

- Jump server or any other intermediate host accessed or used from any of the above
- ~~and when used jump server: sessions to operating~~ systems hosting a SWIFT-related component (including interface, GUI, SWIFT and customer connectors)~~,~~
- network devices protecting the secure zone ~~or to~~
- ~~the virtualisation platform~~ management console (also called the hypervisor manager) of a virtualisation platform hosting SWIFT-related components (including SWIFT and customer connector)
- ~~dedicated and general operator PC and, when used, jump server: sessions to~~ interface applications, GUI and SWIFT or customer connector in the secure zone
- ~~or to~~ applications at the service provider
- ~~secure zone: session to~~ HSM~~, SWIFT-related applications, network devices, and operating systems from dedicated operator PCs~~
- [Advisory A1/A2/A3: ~~Operator sessions to~~ the middleware server (such as an IBM® MQ server or similar) u~~til~~ised for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]

Risk Drivers:

- loss of operational confidentiality
- loss of operational integrity
- password theft

Implementation Guidance

Control Statement:

The confidentiality and integrity of interactive operator sessions that connect to service provider SWIFT-related applications ~~(local or at the service provider)~~ or into the secure zone are safeguarded.

Control Context:

Operator sessions, through the jump server when used with the local or external SWIFT infrastructure, pose a unique threat because unusual or unexpected activity is more difficult to detect during interactive sessions than it is during application-to-application activity. Therefore, it is important to protect the integrity and confidentiality of these operator sessions to reduce any opportunity for misuse or password theft. When used, access to the virtualisation layer (hypervisor manager) must be similarly protected.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- All interactive sessions are protected by a cryptographic protocol (for example, ssh, https with one-way TLS).
- Protocols use a current, commonly accepted cryptographic algorithm (for example, AES[31] or ECDHE[32]), with key lengths in line with the current best practices. More guidelines on cryptographic algorithms that support secure protocols can be found in SWIFT Knowledge Base article 5021566.
- Operator sessions and other session types (for example, admin or maintenance) possess an inactivity lock-out feature that limits the session to the minimal time frame necessary to perform business-as-usual duties.
- If the inactivity lock-out is not implemented at the application level, then it should be implemented at the operating system level of the application, or on the jump server.
- The communication between the jump server (when used) and the SWIFT-related components or underlying systems, is protected using a secure mechanism (for example, one-way or two-way TLS) to support the confidentiality and integrity of the user's connection to the applications or the underlying systems.

[31] Advanced Encryption Standard

[32] Elliptic Curve Diffie-Hellman Ephemeral

2.7 Vulnerability Scanning

Control Type: Mandatory / Advisory for B	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.

In-scope components:

- jump server
- Dedicated operator PCs
- [Advisory: General-purpose operator PCs as per the optional enhancement]
- ~~secure zone:~~ all ~~SWIFT-related applications and operating~~ systems hosting a SWIFT-related component (including interface, GUI, SWIFT and customer connectors)~~, also including dedicated operator PCs~~
- [Advisory: Local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs and their management PCs as per optional enhancement]
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) u~~ti~~sed for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~

Risk Drivers:

- exploitation of known security vulnerabilities

Implementation Guidance

Control Statement:

Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities using an up-to-date, reputable scanning tool and results are considered for appropriate resolving actions.

Control Context:

The detection of known vulnerabilities allows vulnerabilities to be analysed, treated, and mitigated. The mitigation of vulnerabilities reduces the number of pathways that a malicious actor can use during an attack. A vulnerability scanning process that is comprehensive, repeatable, and performed in a timely manner is necessary to continuously detect known vulnerabilities and to allow for further action.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Vulnerability scanning is performed at least annually or after any significant change to the environment (for example, introduction of new servers or components, and network design changes that modify or increase the range of in-scope components).
  - Vulnerability scanning tools are from a reputable vendor and are updated with scan profiles within one month prior to scanning.
  - The most appropriate type of vulnerability scanning (such as using credentials) is selected for the environment. Any administrative credentials used for scanning are appropriately protected.

  - Sufficient risk-based safeguards are in place to minimise any operational impact (for example, running scans in safe mode, or omitting systems that may be negatively affected from the scan).
- Beyond vulnerability identification through scanning, all penetration tests or effective vulnerability tests on or through SWIFT-related services and products are consistent with the SWIFT Customer Testing Policy.
- The outcome of the vulnerability scanning is documented (with restricted access) and analysed for appropriate action and remediation (such as applying security updates in line with control **2.2**).
- Once per quarter, month, or real-time (preferred) scanning is recommended.

Optional Enhancements:

- Vulnerability scanning includes network devices protecting the secure zone~~components~~ (such as routers and switches).
- Vulnerability scanning includes the general-purpose operator PCs used to connect to the local or service provider's SWIFT~~-related~~ infrastructure. As an alternative, security updates are regularly applied on the general-purpose operator PCs. In the latter case, only supported and regularly patched applications are deployed on those PCs.
- Vulnerability scanning possibly includes the local or remote (hosted or operated by a third party, or both) Virtualisation platform that hosts the SWIFT-related VMs.

2.8A Critical Activity Outsourcing

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure the protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.

In-scope components:

- Organisational control is applicable when outsourcing critical SWIFT-related activities to a third party or a service provider.

Note: This control remains strongly recommended even when the activities being outsourced are not critical.

Risk Drivers:

- exposure to sub-standard security practices

Implementation Guidance

Control Statement:

Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.

Control Context:

When critical activities are outsourced to third parties (for example, external IT provider or cloud provider) or service providers (such as a service bureau or a Lite2 for Business Application provider), it is essential that at a minimum, the original standard of care for security is maintained (in addition to adherence to this security control framework) to make sure that no new weaknesses or vulnerabilities are introduced.

Note:

- SWIFT defines the following ~~operations~~ activities, at a minimum, as critical:
  - security management and change management of the hardware and software (including applications, operating system, and underlying virtualised platform or infrastructure) supporting the SWIFT service
  - RMA-related operations
  - accessing sensitive user data (for example, message content)
  - monitoring of events that contain sensitive user data
  - network management and configuration
  - SWIFT-related transaction operations (for example, creation or modification of a financial transaction message within the messaging interface)

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- When outsourcing the SWIFT ~~-related~~ infrastructure (or a part of it) to a third party (such as an external IT provider or a cloud provider such as the Digital Connectivity ~~solution~~Initiative) acting on its behalf, the user remains responsible for the conformance with the security controls of this framework and must seek compliance from that third party.
- When the third party provides shared services to connect no-related SWIFT users, the third party must be registered for the Shared Infrastructure Programme (SIP) or the Alliance Lite2 for Business Applications (L2BA) programme. Users remain responsible for their own infrastructure, organisation, and for

implementing secure data flows toward the provider in line with the provider's specifications. Users are also responsible for monitoring the provider's compliance with the relevant SIP or L2BA programme[33]:

- Service bureaux registered and compliant under the SIP are listed in the SWIFT Partner Programme Service Bureau Directory.
- L2BA providers registered and compliant under the related programme are listed in the Lite2 Business Applications Providers Directory.

- Service Level Agreements (SLAs) and a Non-disclosure Agreement (NDA) are established with any third party or service provider when critical activities have been outsourced. These SLAs define the standard of care under which those critical operations are carried out by the third party or the service provider.
- A risk assessment of the third party is conducted at the start of the engagement, and is reviewed on a regular basis thereafter.

Note: SWIFT expects this control to become mandatory in a future version of this document.

[33] A provider remains listed as long as it is compliant. Should it be de-listed, it would be listed again once compliance is regained.

2.9A Transaction Business Controls

Control Type: ~~Advisory~~Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: ~~Restrict~~ Ensure outbound transaction activity within the expected bounds of normal business.

In-scope components:

- GUI
- ~~secure zone:~~ messaging interface
- ~~secure zone:~~ communication interface
- ~~secure zone:~~ SWIFT and customer connector
- ~~customer connector~~

Note: Components are mentioned as the vector for outbound transaction business, not necessarily ~~controls~~where controls are performed. Transaction activity refers to payment instructions. Reliance on other relevant recent (business) assessment, audit or regulator answers to confirm effectiveness of the control is an option[34].

Risk Drivers:

- business conducted with an unauthorised counterparty
- undetected anomalies or suspicious activity

Implementation Guidance

Control Statement:

Implement transaction detection, prevention, and validation controls to ~~restrict~~ ensure outbound transaction activity ~~to~~ within the expected bounds of normal business.

Control Context:

Implementing business controls that restrict SWIFT transactions to the fullest extent possible reduces the opportunity for the sending (outbound) and, optionally, receiving (inbound) of fraudulent transactions. These restrictions are best determined through an analysis of normal business activity. Parameters can then be set to restrict business to acceptable thresholds based on “normal” activity.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user’s implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Implement controls that will detect, prevent, or additionally validate the flow of transactions against the expected bounds of normal business ~~(payment controls service)~~. **Examples** of potential measures can include any or a combination of the following four elements:
  - (1) limiting traffic outside of business hours
    - Note: This measure may not be applicable to some users: a~~A~~s business hours are organisational and business unit-specific, multiple start and finish times (business hours) may need to be supported or no specific range can be defined for systems used on a 24-hour basis. In cases of 24-

[34] Although reliance on recent certification, audit or assessment is allowed for any CSP control as per the Independent Assessment Framework (IAF), it is even more relevant in this control.

hour centralised SWIFT processing, limit or monitor transactions as appropriate to support business as usual.

- Consider restricting SWIFT transaction submissions and approvals outside of normal business hours[35]. ~~In cases of 24-hour centralised SWIFT processing, monitor transactions as appropriate to support business as usual. Suspicious messages can be blended in with legitimate traffic.~~
- Consider enabling active FIN sessions to business hours only (for example, using automated logical terminal sessions log out at the end of the business day). ~~In cases of 24-hour centralised SWIFT processing, monitor transactions as appropriate to support business as usual.~~
- Suspicious messages can be blended in with legitimate traffic during business hours. Therefore, always limit or monitor transactions as appropriate, to support business as usual activities considering the next elements.

– (2) limiting traffic beyond normal business amount ranges

- Consider restricting SWIFT transactions outside of customer-defined amount limits. Such limits can be specified globally, per region, traffic or known correspondents in line with functionalities offered by the used SWIFT-related interface, application or service. Putting on-hold restricted transactions for additional/off-line validation and approval (in line with separation of duties as per control 5.1) is deemed a valid control.

– (3) performing end-of-day and (possibly) intra-day validations through any or a combination of the following

- Consider i~~I~~mplementing a process to issue and check confirmation messages (for example, to check that the MT 900 and MT 910 confirmations match the transactions which have occurred on the accounts or through potential online queries for intra-day Nostro reconciliation).
- Consider r~~R~~econcilinge the entity's accounting records with end-of-day statement messages (for example, MT 940 and MT 950 or through potential online queries for end-of-day Nostro reconciliation).
- Consider r~~R~~econcilingiation is performed daily (and possibly intra-day)~~between the~~ messages that are sent to/from the back office and to/from the SWIFT Network.

– (4) performing central checks on payments to spot potential abnormal behaviour

- Consider tracking s~~S~~ession numbers within the messaging interface ~~are tracked~~ to make sure that the sequential session numbering is intact with no unexpected gaps.
- Consider m~~M~~onitoring uncharacteristic transactions (for example, exceptionally high amounts or cumulative amounts, unusual beneficiaries, senders, or currencies) based on self-determined criteria.

- ~~•~~ Alternatively, independent reconciliation is undertaken with a user's transaction data securely obtained from a secondary source (either internal or external, such as the SWIFT Daily Validation Reports or other reports from service providers) or by verifying that the transaction is genuine with the emitter or the recipient (or both).
-

Optional Enhancements:

- Application and operating system accounts are restricted from login attempts that occur outside of the expected role-specific operational hours.
- Implement controls to ~~restrict~~ ensure inbound transaction activity within the expected bounds of normal business.
- Implement controls to other sensitive transactions not limited to payments.

[35] Limiting or dully controlling sessions outside of normal business flows can introduce delays allowing to intercept/recall fraudulous transactions before their potential immediate processing and ultimately cash-out.

2.10 Application Hardening

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•		

Control Definition

Control Objective: Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-compatible messaging and communication interfaces, the SWIFT connector and related applications.

In-scope components:

- messaging interface
- communication interface
- GUI
- SWIFTNet Link
- SWIFT connector

Risk Drivers:

- excess attack surface
- exploitation of insecure application configuration

Implementation Guidance

Control Statement:

All messaging interfaces and communication interfaces products within the SWIFT secure zone are SWIFT-compatible. Application security hardening is conducted and maintained on all in-scope components.

Control Context:

Application hardening applies the security concept of “least privilege” to an application by disabling features and services that are not required for normal operations. This process reduces the application capabilities, features, and protocols that may be used during an attack. The process also makes sure that potential default credentials are changed.

In addition, SWIFT runs a Compatible Interface Programme to make sure interfaces are aligned with current practices and to give the customer additional assurance, guarantees, and better visibility regarding individual product capabilities. Upon the successful validation of the test results by the SWIFT Test Authority, the interface is published in the Compatible Register. As per the SWIFT General Terms and Conditions, customers must use a SWIFT-compatible interface.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user’s implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Make sure the messaging and communication interfaces are SWIFT-compatible (the list of compatible interfaces is published in the Compatible Register on www.swift.com).
  - The SWIFT-compatible interface should meet all the security conformance requirements (mandatory and advisory) defined in the SWIFT Compatible Interface Programme.
    - If some security conformance requirements are yet to be met, then the user should upgrade to a SWIFT-compatible interface by implementing at least the minimum mandatory security conformance requirements.
    - The interface provider should be contacted in case of doubts regarding the availability of some security functionalities or their proper configuration and usage.

- All in-scope applications are hardened considering one or more of the following:
  - vendor security, operational or configuration guidance (such as the Alliance Security Guidance)
  - a local or a regulator's standard security configuration, or controls set of the same rigour as the vendor guidance
- At a minimum, the application hardening process should do the following:
  - Change default existing passwords.
  - Disable or remove unnecessary user accounts.
  - Disable or restrict unnecessary components, adaptors, or connectivity methods.
  - Securely configure the adapters, connectivity methods, or remote connections.
  - Remove unnecessary packages.
  - Adjust any default configurations known to be vulnerable.
- Deviations from the selected hardening configuration (that is, a set of rules) are documented along with the justification for the deviation.

Optional Enhancements:

Additional applications installed on the systems that host in-scope components and handle SWIFT-related data are also subject to considered application hardening as per the vendor recommendations.

2.11A RMA Business Controls

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Restrict transaction activity to validated and approved business counterparties.

In-scope components:

- GUI
- ~~secure zone:~~ messaging interface
- SWIFT and customer Connector~~s~~

Note: GUI, connectors, and messaging interface are mentioned as the potential vector for Relationship Management Application (RMA) exchange and reporting.

Risk Drivers:

- business conducted with an unauthorised counterparty

Implementation Guidance

Control Statement:

Implement RMA controls to restrict transaction activity with effective business counterparties.

Control Context:

- Implementing business controls that restrict SWIFT transactions to the fullest extent possible reduces the opportunity for both the sending and receiving of fraudulent transactions. These restrictions are best determined through an analysis of effective business relationships where RMA is a mechanism to prevent unwanted traffic on a service by controlling who can send traffic and what type of messages can be exchanged through Relationship Management Application Plus (RMA+).

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- RMA
  - Appropriate know-your-customer principles and due diligence is performed during the creation and maintenance of RMA relationships.
  - RMA relationships are reviewed annually (at least) to make sure that obsolete (unused, dormant, or unwanted) relationships are analysed and removed or revoked in a timely manner.

Optional Enhancements:

- RMA+

  Restrict the valid RMA relationships to the specific message types that are agreed with the counterparty.
  - ~~***Note***: SWIFT expects this control to become mandatory in a next version of this document.~~

3 Physically Secure the Environment

3.1 Physical Security

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.

In-scope components:

- dedicated and general-purpose operator PC ~~and jump server (when used)~~, including removable equipment
- jump server
- local or remote (hosted or operated by a third party, or both) hardware hosting a SWIFT-related component (including interface, GUI, SWIFT and customer connectors)
- ~~secure zone: all hardware~~
- local or remote (hosted or operated by a third party, or both) hardware supporting virtualisation platform (also referred to as the hypervisor) and hosting SWIFT-related VMs
- [Advisory A1/A2/A3: Middleware server (such as an IBM® MQ server or similar) u~~til~~ised for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- ~~[~~Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~
- Alliance Connect SRX VPN boxes and Alliance Connect Virtual VPN instances

Note: Alliance Connect SRX VPN boxes and ~~the~~ Alliance Connect Virtual~~virtual~~ VPN instances (hosting systems or machines) ~~are generally out of scope, but are expected~~must also~~to~~ be in an environment with appropriate physical controls as described below.

Risk Drivers:

- lack of traceability
- unauthorised physical access

Implementation Guidance

Control Statement:

Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage.

Control Context:

Implementing physical security controls protects against insider and external threats, and reduces opportunistic attacks enabled by access to physical systems.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Security of Removable Equipment
  - Sensitive removable equipment, such as PIN Entry Devices (PEDs), PED keys, SWIFT-related smart cards, USB Tokens, and (time-based) one-time password ((T)OTP) Devices, is supervised or securely stored when not in use.
  - Sensitive removable equipment required for normal continuous operations (for example, hot swappable disks or HSM devices) are hosted in a data centre or, at a minimum, in a locked room.
  - Back-up media (for example, tapes) is physically secured.
- Security of the Workplace Environment
  - Operator PCs are located in a secured workplace environment where access is controlled and granted only to employees and other authorised workers and visitors. A separate physical area for operator PCs to access SWIFT systems is not required.
  - Printers used for SWIFT transactions are located in a secured workplace environment and their access is restricted.
  - USB ports ~~devices~~ and other external access points on operator PCs are disabled to the maximum extent possible, while continuing to support operations (for example, when tokens are required to authenticate users or message operations).
- Security for Remote Workers (for example, teleworkers or "on call" operations staff)
  - A security policy is established to support expected use cases for remote workers. The following items are considered when establishing the policy:
    - physical security of the expected teleworking environment
    - rules for personal equipment used for SWIFT business purposes (for example, personal PCs cannot be used to access the SWIFT infrastructure, however personal mobile devices can be used as a second authentication factor)
    - security during use in public environments
    - security during public and private transport
    - equipment storage
    - unauthorised access to equipment (for example, from family or friends)
    - remote access requirements (recommended VPN with multi-factor authentication)
    - protection of mobile devices used for authentication, such as (T)OTP (recommend enabling password and auto-lock features)
    - compensating controls (for example, virtual desktop preventing local storage, full-disk encryption)
    - reporting of security incidents (for example, theft) while working remotely
- Security of the Server Environment
  - Servers are hosted in a data centre or, at a minimum, in a locked room with limited and controlled access (for example, using access control cards or biometrics).
    - Ideally, servers are rack-mounted. A risk assessment is conducted to determine if a separate and exclusive rack, or the locking of the rack, is appropriate based on the existing data centre physical access controls.
  - The server environment has video surveillance with movement detection and recording equipment. The implementation of video surveillance recording and retention of images comply with applicable laws and regulations[36]. Ideally, images are retained for at least three months.
  - No physical reference to SWIFT on servers (for example, labels).
  - External ports (for example, USB, serial bus) on servers are disabled to the maximum extent possible while still supporting operations.
- Physical Access Logging and Review
  - Physical access to sensitive equipment areas (for example, data centre, secured storage) is logged.
  - Physical access logs are available for audit and investigations, and are retained for a minimum of 12 months and in compliance with applicable laws and regulations.
  - Physical access is promptly revoked (or modified) when an employee changes roles or leaves the organisation.
  - Physical access control lists are reviewed annually (at least).

[36] Such as the "Guidelines 3/2019 on processing of personal data through video devices", local Data Protection Act/code of practice or Laws related to video surveillance

4 Prevent Compromise of Credentials

4.1 Password Policy

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.

In-scope components:

Passwords defined on the following components: ~~login to~~

- dedicated and general-purpose operator PCs
- ~~and~~ jump server ~~(when used)~~
- SWIFT-related components (including interfaces, GUI, SWIFT and customer connectors)
- systems hosting SWIFT-related components ~~secure zone: application and operating system accounts including~~
- network devices ~~that~~ protecting the secure zone
- local or remote (hosted or operated by a third party, or both) virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs and their management PCs
- [Advisory A1/A2/A3: Middleware server (such as IBM® MQ server or similar) u~~tili~~sed for data ~~to~~ exchange between back-office and ~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~
- personal tokens and personal mobile devices used as possession factor for multi-factor authentication (see control **4.2**)

Risk Drivers:

- password cracking, guessing, or other computational compromise

Implementation Guidance

Control Statement:

All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters.

Control Context:

Implementing a password policy that protects against common password attacks (for example, guessing and brute force) is effective for protecting against account compromise. Attackers often use the privileges of a compromised account to move laterally within an environment and progress the attack. Another risk is the compromise of local authentication keys to tamper with the integrity of transactions.

However, it is important to recognise that passwords alone are generally not sufficient in the current cyber-threat landscape. Users should consider this control in close relationship with the multi-factor authentication requirement.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are

not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- A password policy that also covers PIN settings is established, aligned to current industry standards or industry best practices, and defines the following criteria:
  - password expiration
  - password length, composition, complexity, and other restrictions
  - password re-use
  - lock out after failed authentication attempts (and remedy)
  - password requirements modified as necessary for the following specific use cases:
    - in combination with a second factor (for example, one-time password)
    - authentication target (for example, operating system, application, mobile device, or token)
    - type of account (general operator, privileged operator, application-to-application account, or local authentication keys)

  For additional best practice guidelines about password and PIN parameter settings, see SWIFT Knowledge Base articles 5021567 and 5022038.
- The password policy is developed in consideration of known password-based vulnerabilities in the computing environment. For example, requiring a password of 15 or more characters for Windows systems prevents Windows from computing the highly vulnerable LAN Manager (LM) password hash.
- The established password policy is enforced through technical means (for example, through an Active Directory group policy, or within application settings), when possible.
- Effectiveness of the password policy is reviewed regularly (annually, by recommendation).
- System settings related to password management and storage are aligned to industry and vendor best practices (for example, enabling the "NoLMHash" registry setting in Windows).
- Passwords used for secure zone systems are significantly more exposed if the passwords are stored in authentication systems outside of the secure zone (for example, an enterprise Active Directory). Instead, passwords for secure zone systems are, to the fullest extent possible, stored only within the zone (for example, in an Active Directory for production systems) as described in the guidance for the design of the secure zone or another existing secure zone that has similar controls.

***Note*:** Users should implement strong passwords and preferably strong authentication mechanisms for all systems used within the end-to-end transaction chain, and not limit these controls to the SWIFT infrastructure only.

4.2 Multi-Factor Authentication

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Prevent that a compromise of a single authentication factor allows access into SWIFT-related systems or applications by implementing multi-factor authentication.

In-scope components (depending on implementation):

- dedicated operator PC login
- ~~operator~~ access to jump server
- ~~operator~~ login process to the messaging interface (including a related hosted database), communication interface, SWIFT and customer connector (including a related hosted database) or a service provider SWIFT-related application
- login process to (operating) systems hosting the messaging interface (including a hosted database), SWIFT and customer connector (including a related hosted database) and communication interface or a service provider SWIFT-related application
- access to the remote SWIFT infrastructure (hosted or operated by a third party, or both)

Risk Drivers:

- credential replay
- password cracking, guessing, or other computational compromise
- password theft

Implementation Guidance

Control Statement:

Multi-factor authentication is used for interactive user access to SWIFT-related components or applications and operating system accounts.

Control Context:

Multi-factor authentication requires the presentation of two or more of the following common authentication factors:

- knowledge factor: something the operator knows (for example, a password)
- possession factor: something the operator has (for example, connected USB tokens or smart cards, or disconnected tokens such ~~as~~ as a (time based) one-time password (T)OTP generators ~~-~~ or application storing a cryptographic private key that runs on~~using~~ another device like operator's mobile phone, RSA token or Digipass)
- inherence factor: something the operator is (for example, biometrics such as fingerprints, retina scans, or voice recognition)

Implementing multi-factor authentication provides an additional layer of protection against common authentication attacks (for example, shoulder surfing, password re-use, or weak passwords) and provides further protection from account compromises for malicious transaction processing. Attackers often use the privileges of a compromised account to move laterally within an environment and to progress an attack.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- When implementing multi-factor authentication, the following principles apply:
  - When based on a knowledge factor (typically a password) combined with a possession factor (a mobile device), the device used for the second factor must not be the same as the device used to enter the first factor. As such, using an app to generate the second factor on the same device/PC used to enter the first factor (password) is not sufficient to access the local SWIFT systems.
    - Second factor solutions based on a possession factor include (but are not limited to) TOTP, RSA SecurID, Digipass, Mobile App, Transaction Authentication Number (TAN) Table, and personal USB token. The solution should be selected per the user's risk management.
  - An inherence factor is more safely combined with a possession factor than with a knowledge factor.
- Multi-factor authentication is implemented on one authentication stage/step (at minimum) encountered by the system administrator or the end user when accessing a SWIFT application or the hosting system.
  - Operating system administrators when accessing the hosting system:
    - at the secure zone boundary (jump server)
    - at the dedicated operator PC login (within the secure zone)
  - End users (in descending order of security robustness) when accessing the SWIFT application:
    - on the individual SWIFT applications (the browser-based GUI, the messaging interface, or the communication interface)
    - at the secure zone boundary (jump server)
    - at the dedicated operator PC login (that is, within the secure zone)
- Multi-factor authentication is implemented for remote user administrative access, generally for VPN authentication.
- Multi-factor authentication systems are significantly more exposed if the authentication credentials are stored outside of the secure zone (for example, within an enterprise Active Directory). If possible, then the authentication system that supports the multi-factor solution is located within the secure zone.
- The presented authentication factors are individually assigned and support the individual accountability of access to services, operating systems, and applications.
- If single sign-on (for example, SAML) is implemented, then a second factor is still required at the login or at a later stage.
- Multi-factor authentication must be presented when accessing (at least for transaction processing[37]) a SWIFT-related service, application, or component that is operated by a service provider (such as a service bureau, an L2BA provider, or an intermediate actor).

***Note*:** All SWIFT and SWIFT-compatible third-party vendor messaging and communication interfaces must support or embed multi-factor authentication.

Considerations for alternative implementations:

When the device used for the second factor is the same as the one used to enter the first factor, additional mitigations must be identified and implemented in line with a user risk assessment.

The objective of the risk assessment is to evaluate and keep potential risks under user's risk appetite when combining factors in case of loss, theft or compromise of such device. Mitigations can include technical measures (such as enforcing a PIN or a password to unlock an application linked with the registered device, application that generates a one-time string; limiting the accessed functions depending on the device level of trust; requiring additional factor, such as a biometric factor to unlock cryptographic private key(s) used as possession factor, for most sensitive functions,…) and include as well complementary procedural requirements (such as Policy asking end user to immediately contact a security operations centre -SOC- to block or put on-hold any potential access or transaction performed through this lost, stolen or potentially compromised device).

[37] such as ~~posting,~~ creating, submitting, approving or modifying transactions or user entitlements.

5 Manage Identities and SeparateSegregate Privileges

5.1 Logical Access Control

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Enforce the security principles of need-to-know access, least privilege, and separationsegregation of duties for operator accounts.

In-scope components:

User, operator or management accounts defined on the following components:

- All operator accounts (for example, on a local or remote virtualisation platform and their management PCs, also referred to as the hypervisor, hosting SWIFT-related VMs and , on those VMs themselves
- , jump server
- , dedicated operator PCs,
- operating systems hosting interfaces, GUI, SWIFT and customer connectors or service provider SWIFT-related, applications and on those , interfaces, GUI, connectors or service provider SWIFT-related applications
- and HSM)
- network devices protecting the secure zone
- SWIFTNet Online Operations Manager (O2M) on swift.com
- [Advisory: All operator accounts on the customer connector and middleware server (such as IBM® MQ server or similar) utilised for data to exchange between back-office andwith SWIFT-related components]

Risk Drivers:

- excess privilege or access
- segregation separation of duty violation
- unauthorised access

Implementation Guidance

Control Statement:

Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation separation of duties.

Control Context:

Applying the security principles of (1) need-to-know, (2) least privilege, and (3) segregation separation of duties is essential to restricting access to the local SWIFT infrastructure. Effective management of operator accounts reduces the opportunities for a malicious person to use these accounts as part of an attack.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be

considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

A logical access control policy is documented and enforced based on the following principles:

- Need-to-know.
  - Only operators (end users and administrators) who have a continuing requirement to access the secure zone are permitted to have accounts within the secure zone.
  - Privileges are only assigned to an operator with a validated need-to-know (for example, system set-up makes sure that operators only have access to the information, files, and system resources necessary for their defined tasks). Access to other system functions is disabled.
- Least Privilege.
  - The system set-up makes sure that user and administrator privileges are controlled in a way that allows all privileges to be tailored to individual needs.
  - Accounts are granted only to privileges that are required for normal, routine operation. Additional privileges are only granted on a temporary basis.
- ~~Segregation~~ Separation of Duties and Four-Eyes.
  - Vendor documented guidance on role separation is followed in vendor-specific documentation.
  - Sensitive duties are separated. This means that some roles cannot be represented by the same individual, such as:
    - Transaction submission and transaction approval
    - Application Administrator and security officer roles
    - Network and operating system administrators.
  - Sensitive permissions are separated to prevent by-passing the Four-Eyes principle. At a minimum, this requirement applies to access control and security configuration operations on the following components: Messaging and Communication Interface, HSMs, SWIFTNet Online Operations Manager, and Secure Channel.
- Account Review and Revocation
  - Privileges (including those delegated to providers) are promptly revoked when an employee changes roles or leaves the organisation (or the provider). Privileges assignment must ensure continuous accountability and traceability.
  - Accounts (including those delegated to providers) are reviewed at least annually ~~(ideally more frequently)~~ and adjusted as required to continuously ensure accountability and traceability of accounts assignment~~enforce access security principles~~.
- An emergency procedure to access privileged accounts is documented for use when authorised people are unavailable due to unexpected circumstances:
  - Any operational use of the procedure is logged.
  - Access to the emergency privileged accounts is controlled. Usage is logged ensuring accountability and traceability and the password is changed after emergency use.

5.2 Token Management

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure the proper management, tracking, and use of connected and disconnected hardware authentication or personal tokens (when ~~if~~ tokens are used).

In-scope components:

- connected and disconnected hardware authentication or personal tokens used for SWIFT operations or secure zone access
- PIN Entry Device (PED) used for HSM operations

Risk Drivers:

- authentication token theft
- lack of traceability
- HSM management misused

Implementation Guidance

Control Statement:

Connected and disconnected hardware authentication or personal tokens are managed appropriately during their assignment, distribution, revocation, use, and storage.

Control Context:

The protection of connected and disconnected hardware authentication or personal tokens is essential to safeguarding the related operator or system account. It also reinforces good security practice by providing an additional layer of protection from attackers.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- A controlled process is used for the assignment and distribution of connected and disconnected hardware or personal tokens used for SWIFT operations (for example USB token, HSM token, smart card).
- Token assignment, including those delegated to a provider, is reviewed at least annually (more frequently is recommended ~~preferred~~).
- Personally assigned hardware tokens, including those delegated to a provider, are revoked when the individual no longer requires access and should be recalled (for possible disposal or reassignment as appropriate).
- A record is maintained of assigned hardware token ownership.
- Hardware tokens are physically removed from the system and secured or supervised when not in use.
- When a remote PED is used, the following security practices apply:
  - PED keys must be stored and only accessible by relevant staff (originals and copies should be stored in a safe with access tracking)
  - Although the HSM PED keys are not personally assigned, usage should be controlled, tracked and monitored. In case a PIN is set on the PED keys and a person with access to these keys and PIN is leaving the company, the PIN codes should be changed

- The flows to the HSM must be secured as per the Alliance Security Guidance considering also the CSP FAQ (SWIFT Knowledge Base article 5021823) to properly establish and manage the connection.

5.3A Staff Screening~~Vetting~~ Process

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: To the extent permitted and practicable, e~~E~~nsure the trustworthiness of staff operating the local SWIFT environment by performing regular staff screening ~~personnel vetting in line with applicable local laws and regulations~~.

In-scope components:

- All staff (such as employees, agents, consultants and contractors) with operational (maintenance or administration) access to SWIFT-related systems, SWIFT and customer connector or middleware servers and local or remote virtualisation platform hosting SWIFT-related VMs, SWIFT and customer connector VMs or middleware server VMs.

Risk Drivers:

- untrustworthy staff or system operators

Implementation Guidance

Control Statement:

Staff operating the local SWIFT infrastructure are screened~~vetted~~ prior to initial appointment in that role and periodically thereafter.

Control Context:

A staff ~~vetting~~ screening process with internal or external clearance, provides additional assurance that operators or administrators of the local SWIFT infrastructure are trustworthy, and reduces the risk of insider threats.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

To the extent permitted under applicable laws and regulations[38], and considering local practices and ~~to the extent the~~ available information ~~is available~~, the following guidelines and specified verifications are recommended:

- All in-scope staff are screened~~vetted~~ at least every 5 years.
  - For those already in the role and not yet screened~~vetted~~, a catch-up process is gradually organised as part of the periodic ~~vetting~~ screening (sometimes also referred to as re-screening~~vetting~~)
- The ~~vetting~~ screening process for initial employment includes the following verifications ~~(to be conducted in line with applicable local laws and regulations)~~:
  - Identity verification
  - Confirmation of full details of qualifications
  - Confirmation of previous employment history
  - Details of any past or pending civil or criminal proceedings against the employee
  - Validation of any involvement in external businesses that could result in a conflict of interest

[38] Including, where applicable, social concertation

- Financial credit verification

- The periodic ~~vetting~~ screening process includes the following verifications ~~(to be conducted in line with applicable local laws and regulations)~~:
  - Details of any pending civil or criminal proceedings against the employee
  - Validation of any involvement in external businesses that could result in a conflict of interest
  - Financial credit verification

Note: in case of staff not directly employed by the SWIFT user (such as agents, contractors or consultants), the screening can fall under contractual obligation between the SWIFT user and the employer.

5.4 Physical and Logical Password Storage

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Protect physically and logically the repository of recorded passwords.

In-scope components:

Repository recording aAccounts and passwords defined on the following components:

- dedicated and general-purpose operator PC ~~and, when used, jump server: for operating system access~~
- jump server
- ~~dedicated and general-purpose operator PC and, when used, jump server: interactive user session~~
- SWIFT-related components (including interfaces, GUI, SWIFT and customer connectors)
- systems or virtual machines hosting SWIFT-related components
- ~~secure zone: all applications, operating systems,~~ HSM and related tokens~~, and~~
- network devices~~components~~ protecting the secure zone
- local or remote (hosted or operated by a third party, or both) virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs
- [Advisory A1/A2/A3: Middleware server (such as IBM® MQ server or similar) used for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
-
- ~~[Advisory A4: Customer connector]~~
- SWIFTNet Online Operations Manager (O2M) on~~and~~ swift.com

Risk Drivers:

- password theft

Implementation Guidance

Control Statement:

Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-to-know basis.

Control Context:

The secure storage of recorded passwords (repository) makes sure that passwords are not easily accessible to others, thereby protecting against simple password theft. Common unsecure methods include, but are not limited to: recording passwords in a spreadsheet or a text document saved in cleartext on a desktop, or in a shared directory, or a server, saved on a mobile phone, written/printed on a post-it or a leaflet.

This control covers the storage of emergency, privileged or any other account passwords. All accounts have to be considered because (i) combination of compromised, not-privileged, accounts, such as transaction creator account and approver account can be damageable, and (ii) even monitoring accounts provide valuable information during the reconnaissance time.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Passwords written on physical media are protected through:
  - placing inside a sealed, tamper-evident security envelope
  - storing in a safe
  - logging the access to the storage location and which account passwords have been accessed.
- Passwords stored logically (digitally) are protected through:
  - Encryption-at-rest or obfuscation (that is, no plain text storage),
  - Authenticated access to the storage location, ideally with access logging.
- Passwords are not recorded in user manuals or other operational ~~material~~ means unless the password is stored in line with the guidance above.
- If emergency access is granted to an operator who, under normal conditions, would not have access, then the password is changed immediately thereafter, and optionally, also the combination to the storage safe.
- Passwords are not hardcoded in scripts or other software code.

Optional Enhancement:

The safe is certified through, for example, Underwriters Laboratories (UL) Class TL or EN-1143-1 certification.

6 Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure that local SWIFT infrastructure is protected against malware and act upon results.

In-scope components:

Anti-malware software is implemented on Windows operating systems of the below components:

- dedicated and general-purpose operator PC~~ and when used jump server - Windows operating systems~~
- jump server
- Management PCs of~~en~~ a local or remote (hosted or operated by a third party, or both) virtualisation platform
- ~~secure zone: SWIFT-related~~ systems hosting a SWIFT-related components (including interface, GUI, SWIFT or customer connector)~~ervers - Windows operating systems~~
- [Advisory A1/A2/A3: Middleware server (such as IBM® MQ server or similar) u~~ti~~lised for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components~~ - Windows operating systems~~]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~

Risk Drivers:

- execution of malicious code
- exploitation of known security vulnerabilities

Implementation Guidance

Control Statement:

Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions.

Control Context:

Malware is a general term that includes many types of intrusive and unwanted software, including viruses. Anti-malware technology (a broader term for anti-virus) is effective in protecting against malicious code that has a known digital or behaviour profile.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- On-access anti-malware scanning (also known as real-time or background scanning) is performed on all in-scope systems. On-demand full scanning is scheduled at least on a weekly basis for operator PCs (ideally on a daily basis). On-demand full scanning should be scheduled regularly for servers in line with business and operational constraints. For performance reasons full scans are performed at times of low usage, outside of business hours, or both.

- The scope of the scanning should include all files of the systems in scope. Exclusion of elements or directory from scanning is subject to risk assessment considering user's infrastructure set-up, internal security requirements and policies, the product capabilities and the following principles:
  - Software (such as exe, libraries, scripts) and static data (such as configuration files) are expected to be scanned on-access or at installation, and regularly thereafter, when complemented with a run-time integrity mechanism (in line with the software integrity check depicted in control 6.2) allowing the identification of file changes or unexpected additions.
  - Database server content (data files) can be excluded from the scanning when the data has been checked, validated, and scanned at least once before being stored.
- Anti-malware software from a reputable vendor is installed on all computing platforms and updated in line with the scanning frequency.
- Systems that fail to update their profiles or run scheduled scans are detected and corrected.
- Anti-malware software is tested for compatibility with the operational environment.
- Anti-malware software is configured in prevent mode if possible, after assessing for operational impact. It is recommended to configure the anti-malware software to quarantine suspicious files and to raise an alarm to the user's security department instead of immediately deleting them. This allows the user's security department to investigate the alert and possibly prevent future 'false positives' while allowing the recovery of files if it is confirmed that they are legitimate.
- Files to be sent should be scanned at least once at any stage/step of their internal processing and, ideally, as close as possible to their transfer into the SWIFT network. This is to make sure that such files do not contain viruses or malware that may create risks for the sender, for SWIFT, or for the receiver.
- Endpoint Protection Platform (EPP) solution, combined or not with Endpoint Detection and Response (EDR) offering similar control on the infrastructure can be considered as a valid implementation.

Optional Enhancements:

- Anti-malware systems use a combination of signature-based and heuristic-based capabilities.
- Anti-malware solutions are, when technically possible, implemented on non-Windows systems.
- 'On-demand full scanning' on servers is scheduled to be performed at least on a weekly basis.

6.2 Software Integrity

Control Type: Mandatory / Advisory for A4	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	

Control Definition

Control Objective: Ensure the software integrity of the SWIFT-related ~~applications~~ components and act upon results.

In-scope components:

- ~~Secure zone:~~ SWIFT connector
- ~~Secure zone:~~ GUI to the messaging and communication interface
- ~~Secure zone:~~ messaging interface
- ~~Secure zone:~~ communication interface
- ~~Secure zone:~~ RMA
- ~~Secure zone:~~ SNL
- [Advisory A4: Customer connector]

Risk Drivers:

- unauthorised system changes

Implementation Guidance

Control Statement:

A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related ~~applications~~ components and results are considered for appropriate resolving actions.

Control Context:

Software integrity checks provide a detective control against unexpected modification to operational software.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Software integrity checks are conducted on in-scope components upon start-up, and additionally at least once per day.

  Options for implementation:

  – Integrated in the product
  – Third-party file integrity monitoring (FIM) tool
- Integrity check of downloaded software is conducted through verification of the checksum at the time of its deployment.

Optional Enhancements:

- An integrity check is performed in memory.
- An integrity check is performed at the operating system level.
- File Integrity Monitoring covers the products with integrated mechanisms.

- Systems within the secure zone implement application allow listing on the operating system, which allows only known and trusted applications to be executed.

6.3 Database Integrity

Control Type: Mandatory / Advisory for A4	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	

Control Definition

Control Objective: Ensure the integrity of the database records for the SWIFT messaging interface or the customer connector and act upon results.

In-scope components:

- databases for messaging interface products, including a related hosted database
- databases for customer connector, including a related hosted database

Note: this requirement is ~~not relevant for Architecture A3 and~~ not applicable for Architecture A1 if the infrastructure does not include a messaging interface and for Architecture A4 if there is no database linked to the customer connector.

Risk Drivers:

- loss of sensitive data integrity

Implementation Guidance

Control Statement:

A database integrity check is performed at regular intervals on databases that record SWIFT transactions and results are considered for appropriate resolving actions.

Control Context:

Database integrity checks allow unexpected modification to records stored within the database to be detected.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Database integrity check functionality is enabled to make sure integrity at record level (checksum or signature of the records) and confirm that there are no gaps in sequential transaction numbering.

  Options for implementations:

  - Integrated into the messaging interface application
  - Integrated into the database product where the related hosted database, including its supporting server, is protected similarly to a SWIFT-related component (see the CSP FAQ - SWIFT Knowledge Base article 5021823- for the relevant controls to consider).

Optional Enhancements:

- A full database integrity check is performed at regularly timed intervals, ideally every two weeks.
- The integrity check performs a full referential check on all records (for example, no orphan records between tables) and searches for any unexpectedly deleted records.
- A dedicated database instance is used for SWIFT purposes.

6.4 Logging and Monitoring

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Record security events and detect anomalous actions and operations within the local SWIFT environment.

In-scope components:

- Data exchange layer: network
- Operating system of a dedicated and general-purpose operator PC
- ~~, or, when used,~~ jump server
- SWIFT-related components (including interfaces, GUI, SWIFT and customer connectors)
- systems or virtual machines hosting SWIFT-related components
- ~~Secure zone: SWIFT connector~~
- ~~Secure zone: GUI to the messaging and communication interface~~
- ~~Secure zone: all server applications and operating systems~~
- ~~Secure zone:~~ network devices protecting the secure zone and HSM
- ~~Secure zone:~~ database linked to a messaging interface or a customer connector
- authentication or authorisation servers, or both, controlling accesses to the secure zone
- Local or remote (hosted or operated by a third party, or both) Virtualisation platform (also referred to as the hypervisor) hosting SWIFT-related VMs
- [Advisory A1/A2/A3: Middleware server (such as IBM® MQ server or similar) ~~uti~~used for data~~to~~ exchange between back-office and~~with~~ SWIFT-related components]
- [Advisory A4: other Middleware server (such as an IBM® MQ server or similar) than customer connector used for data exchange between back-office and SWIFT-related components]
- ~~[Advisory A4: Customer connector]~~

Risk Drivers:

- lack of traceability
- undetected anomalies or suspicious activity

Implementation Guidance

Control Statement:

Capabilities to detect anomalous activity are implemented, and a process or tool is in place to ~~frequently~~ keep~~store~~ and review logs.

Control Context:

Developing a logging and monitoring plan is the basis for effectively detecting abnormal behaviour and potential attacks and support further investigations. As the operational environment becomes more complex, so will the logging and monitoring capability needed to perform adequate detection. Simplifying the operational environment will enable simpler logging and monitoring.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are

not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- Overall goals for logging and monitoring:
  - Implement a plan to log security-relevant activities and configure alarms for suspicious security events (when supported by the application).
  - Implement a plan to monitor security events in logs and to monitor other data (for example, real-time business activities through the GUI), and establish a plan to treat reported alarms.
  - Support investigations and forensics in case of potential breach through log retention, in line with applicable laws and regulations.
- ~~All logging and monitoring activity complies with applicable laws and regulations, and employment contracts which supersede other implementation guidance.~~
- Logging:
  - Logging capabilities are implemented to detect and support analysis of abnormal usage within the secure zone and any attempts to undermine the effectiveness of controls within the secure zone.
  - Logs provide traceability of account usage to the appropriate individual.
  - ~~Messaging and communication interface application audit logs are retained for no less than 12 months and are sufficiently protected from an enterprise administrator-level compromise (for example, log files are transferred to a separate system with different system administrator credentials).~~
  - ~~Operator PC, firewall, and database audit logs are retained for no less than 31 days.~~
  - Minimum logs to be recorded include:
    - Command-line history for privileged operating system accounts on servers
    - Messaging and communication interface application and operating system logs which detail abnormal system behaviour (for example, activity outside normal business hours, multiple failed login attempts, authentication errors, changes to user groups)
    - Firewall logs
    - Database logs (if available, and as a minimum in the case of hosted database solutions).
- Monitoring:
  - Procedures are in place to identify suspicious login activities into any privileged operating system or application accounts within the secure zone.
  - Monitoring processes are in place to review server, application, and database monitoring data of the secure zone either daily through human review or through automated monitoring with alerting.
  - Monitoring processes are in place to review network-monitoring data on a regular basis.
  - Unusual or suspicious activity is reported for further investigation to the appropriate security team.
- Log retention:
  - All logging and monitoring activities comply with applicable laws, regulations, and employment contracts which supersede other implementation guidance.
  - Messaging and communication interface application audit logs are retained for no less than 12 months and are sufficiently protected from an enterprise administrator-level compromise (for example, log files are transferred to a separate system with different system administrator credentials).
  - Operator PC, firewall, and database audit logs are retained for no less than 31 days (it is recommended to extend firewall and database audit logs retention to three months and possibly 12 months to support longer investigations).
  - Audit logs captured on other identified in-scope components, at application level or system level, are retained for no less than 12 months.
  - Prevent audit log loss by considering a range of configurable choices when log storage is to be exhausted. As examples, such choices can include log rotation, degraded mode or ignoring some events.

Optional Enhancements:

- A centralised logging capability is implemented, minimising the number of log locations to be inspected.
- Session recording is implemented to record all activity conducted by privileged accounts on SWIFT secure zone servers.

6.5A Intrusion Detection

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	

Control Definition

Control Objective: Detect and contain~~prevent~~ anomalous network activity into and within the local or remote SWIFT environment.

In-scope components:

- network (data exchange layer reaching the SWIFT-related components and inside the secure zone)
- remote (hosted or operated by a third party, or both) virtualisation platform supporting the user SWIFT environment

Risk Drivers:

- undetected anomalies or suspicious activity

Implementation Guidance

Control Statement:

Intrusion detection is implemented to detect unauthorised network access and anomalous activity.

Control Context:

Intrusion detection systems are most commonly implemented on a network (NIDS)[39] – establishing a baseline for normal operations and sending notifications when abnormal activity on the network is detected. As an operational network becomes more complex (for example, systems communicating to many destinations, internet access), so will the intrusion detection capability needed to perform adequate detection. Therefore, simplifying network behaviour is a helpful enabler for simpler and more effective intrusion detection solutions.

Host intrusion detection systems (HIDS) are intended to protect the individual system on which they are implemented and to detect network packets on its network interfaces, similar to the way an NIDS operates.

Intrusion detection systems (NIDS or HIDS) often combine signature- and anomaly-based detection methods. Some systems can respond to any detected intrusion (for example, terminating the connection).

Endpoint detection and response (EDR) is an emerging technology that addresses the need for continuous monitoring and response to advanced threats by detecting suspicious activities and (traces of) other problems on hosts, and on endpoints. This technology is more frequently combined with endpoint protection platform (EPP) that operates at the device level.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- The intrusion detection system is configured to detect anomalous activity within the secure zone and at the boundary of the secure zone. This can be achieved through NIDS, HIDS, or both depending on the network configuration. (For example, large VLAN would better benefit from NIDS; isolated island ~~segregating~~ separating systems may benefit from HIDS. The EDR solution can also be considered.
- Network activity to be tracked for intrusion detection analysis may include:
  - Inbound and outbound connections during non-business hours
  - Unexpected connections from the secure zone towards other systems within or outside of the perimeter of the SWIFT or customer secure zone

[39] Network Intrusion and Detection System

- Unexpected port or protocol use (for example, P2P)

- The system has a repeatable process to regularly update known intrusion signatures.
- If an intrusion is detected, then an alarm is raised and, if the tool permits, a defence mechanism is triggered manually or automatically.
- Detected intrusions are managed through the standard incident response process.

Optional Enhancement:

- Intrusion detection systems can inspect encrypted flows.

Considerations for alternative implementations:

Institutions with a high level of security information and event management (SIEM) maturity within their organisation may consider extending, as stated in control 6.4, their SIEM for real-time analysis of network and systems intrusion.

7 Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure a consistent and effective approach for the management of cyber incidents.

In-scope components:

- organisational control

Risk Drivers:

- excess harm from deficient cyber readiness

Implementation Guidance

Control Statement:

The user has a defined and tested cyber-incident response plan.

Control Context:

Availability and adequate resilience is of key importance to the business. In this respect, defining and testing a cyber-incident response plan is a highly effective way of reducing the impact and duration of a real cyber incident. As lessons are learnt either by testing this plan, or through real incidents, it is essential to apply these learnings and improve the plan. Planning for the sharing of threat and incident information is also critical in helping the broader financial community to implement effective protection against cyber attacks.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- The user has developed and annually updates a cyber-incident response plan. A formal back-up and recovery plan exists for all critical business lines to support incident response activities.
  - The cyber-incident response plan includes up-to-date contact details (internal and external when using third parties or service providers) and escalation timers. Such a plan is based, as a guide, on ~~has to incorporate~~:
    - The Cyber Security Incident - Recovery roadmap that provides a non-exhaustive list of steps or actions that a customer must follow in case of a cyber-security breach including the need to revert to ~~and refer to~~ SWIFT Support. Details are outlined in the SWIFT-ISAC Bulletin #10047.
    - Internal security policies, laws, and regulations within a user's jurisdiction must be adhered to and considered when planning a cyber-incident response.
- As a minimum, the plan is reviewed on an annual basis, and tested at least every two years to make sure safe recovery of critical business operations with minimised outage time after a cyber-security incident.
- The cyber-incident response plan includes steps to:
  - Promptly notify the appropriate internal stakeholders and leadership.
  - Promptly notify the relevant external organisational stakeholders (typically, regulator(s), supervisor(s), law enforcement authorities).

- Promptly notify the SWIFT Customer Support Centre through the default channel and to comply with other obligations applicable to users in case of a security incident including the obligation to cooperate and provide forensic support~~materials~~ as may be required by SWIFT.
- Promptly contain or isolate the impacted system to limit the exposure of the attack while still being able to identify rogue activities.
- Involve skilled cyber-security professionals to identify and address the cyber incident. It is the user's responsibility to take prompt corrective action to investigate, clean the full infrastructure, and resume secure operations as soon as possible.
- Review the correctness of the user current attestation(s) and, as applicable under the SWIFT Security Controls Policy, invalidate such attestation(s) and submit new attestation(s).
- Conduct post-incident problem analysis to identify and remediate vulnerabilities.
- Fully document the incident.

- The user has a documented plan for the timely sharing of threat information to intelligence-sharing organisations, law enforcement, local regulators (as required in each user's jurisdiction) and to SWIFT. Sharing threat information may potentially support root cause analysis and sharing anonymous Indicators of Compromises (IOC) with the community.
- Information to be shared is first evaluated to make sure compliance with applicable laws and regulations (for example, privacy of personal data, confidentiality of investigations) and protects against the unintended sharing of sensitive data or data not relevant to the incident.
- The user can consume threat intelligence shared by SWIFT, for example in the form of IOCs.
- The user has procedures in place to:
  - Make sure the information is distributed to the correct contacts within the organisation,
  - Block traffic to/from IP-addresses/URLs mentioned in the IOCs.

Optional Enhancement:

- The user integrates the SWIFT ISAC automated feed solution in the environment.

7.2 Security Training and Awareness

Control Type: Mandatory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Ensure all staff are aware of and fulfil their security responsibilities by performing regular ~~security training and~~ awareness activities, and maintain security knowledge of staff with privileged access.

In-scope components:

- All staff (such as employees, agents, consultants and contractors) with access to SWIFT-related systems (as user~~usage~~ or for~~,~~ maintenance or administration)
- All staff (such as employees, agents, consultants and contractors) with privileged access to SWIFT-related systems (for maintenance or administration)

Risk Drivers:

- increased security risk from improperly trained staff

Implementation Guidance

Control Statement:

Annual security awareness sessions are conducted for all staff members with access to SWIFT-related systems. ~~including~~ All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion)~~role-specific training for SWIFT roles with privileged access~~.

Control Context:

A security training and awareness programme encourages conscious and appropriate security behaviour of employees and administrators, and generally reinforces good security practice. In addition, it is particularly important that privileged access users have and maintain appropriate knowledge and expertise.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- All ~~S~~staff with access to SWIFT-related systems complete annual security awareness or~~and~~ training. Topics may include:
  - SWIFT-related products and services training (for example, through SWIFTSmart which is available to all users)
  - Cyber-security threat awareness within the financial services industry or relevant to the staff member's role and responsibilities
  - Risks related to internet usage or deployment in the cloud
  - Password security and management
  - Device security
  - Safe operating habits (for example, spam and phishing, including "spear[40]" phishing identification, downloading files, browsing practices)
  - Reporting of suspicious events and activities
  - ~~Detection and response to cyber incidents in line with the organisation's response plan~~
  - Internal or external programme that optionally allows staff to obtain and maintain certification.

[40] Spear phishing is an e-mail or electronic communications scam targeted towards a specific individual, organisation or business.

- In addition, all staff with privileged access maintain their knowledge and expertise in line with their role and responsibilities by considering training or other learning activities that may include topics like:
  - Cyber risks awareness linked to their technologic or SWIFT-related environment (for example, through IOCs published by SWIFT) to develop best practice and processes
  - Administering and securing devices and other used systems
  - Detection and response to cyber incidents in line with the organisation's response plan
  - Internal or external programme that optionally allows staff to obtain and maintain certification.
- Training is delivered through the most appropriate channel, including computer-based training, classroom training, and webinars.

~~People who have access to, for example, SWIFT applications, data, certificates, and network, have an adequate knowledge level and are aware of the relevant cyber risks (for example, through IOCs published by SWIFT), best practice behaviours, and processes.~~

Optional Enhancement:

- Social engineering testing, including fake phishing e-mail campaigns, is performed to challenge and enhance security awareness.

7.3A Penetration Testing

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Validate the operational security configuration and identify security gaps by performing penetration testing.

In-scope components:

- ~~all hardware, software, and network of dedicated and g~~General-purpose operator PCs ~~-~~or, when used, jump servers used to access the secure zone
- Dedicated operator PCs
- Data exchange layer (the entry points to the secure zone or flows established to the secure zone components should be considered)
- ~~Customer connector~~
- SWIFT-related components (including interfaces, GUI, SWIFT and customer connectors)
- systems or virtual machines hosting SWIFT-related components
- network devices protecting the secure zone~~Secure zone: all hardware, software, and network components (in line with the SWIFT Customer Testing Policy, SWIFT-specific applications and SWIFT-central services such as SWIFTNet InterAct, FileAct FIN, SWIFTNet Instant or WebAccess are not in scope)~~
- Remote (operated by a third party) Virtualisation Platform (also referred to as the hypervisor) hosting SWIFT-related VMs and the related management PCs

Note: Tests are performed in line with the SWIFT Customer Testing Policy. As such, SWIFT-specific applications and SWIFT-central services such as SWIFTNet InterAct, FileAct, FIN, SWIFTNet Instant or WebAccess are not to be tested.

Risk Drivers:

- Unknown security vulnerabilities or security misconfigurations

Implementation Guidance

Control Statement:

Application, host, and network penetration testing is conducted towards the secure zone and the operator PCs or, when used, the jump server.

Control Context:

Penetration testing is based on simulated attacks that use similar technologies to those deployed in real attacks. It is used to determine the pathways that attackers might use, and the depth to which the attackers may be able to access the targeted environment. Conducting these simulations is an effective tool for identifying weaknesses in the environment which may require correction, improvement, or additional controls.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- The organisation uses a risk-based approach to determine the preferred scope (for example, the secure zone, or a specific server including potential other services supporting the secure zone), method (for example by sharing or not the internal structure, design or implementation) and attack origin (for example, internal, from within or outside the secure zone, or external attack) for the test.

- Penetration testing is performed at least every 2 years, and ideally as well after significant changes to the environment (for example, introduction of new/different servers, new operating systems, underlying technology such as virtualisation or new network device technology, network design change).
- Penetration testing is carefully planned and performed to avoid potential availability or integrity impacts.
- Penetration testing is performed by expert staff independent from the team in charge of the SWIFT infrastructure (internal Red Team or external resources).
- Network devices~~component~~ and host penetration testing (for example, rule bases and configurations review) are performed in the service production environment or in a pre-production environment replicating the live environment.
- Sufficient safeguards are in place to minimise any operational impact from conducting the penetration test.
- The outcome of the penetration testing is documented (with restricted access) and used as an input for the security update process.

Note: The CSP FAQ (SWIFT Knowledge Base article 5021823) provides additional details on the scoping and the testing scenarios to consider.

Optional Enhancement:

Penetration testing is performed on SWIFT-specific applications while adhering to the SWIFT Customer Testing Policy. This SWIFT-specific application penetration testing is performed in the testing environment to avoid potential availability or integrity impacts.

7.4A Scenario Risk Assessment

Control Type: Advisory	Applies to architecture:	A1	A2	A3	A4	B
		•	•	•	•	•

Control Definition

Control Objective: Evaluate the risk and readiness of the organisation based on plausible cyber-attack scenarios.

In-scope components:

- Organisational control (people, processes, and infrastructure) to be also met by a third party operating a remote virtualisation platform (also known as hypervisor) that hosts SWIFT-related VMs.

Risk Drivers:

- excess harm from deficient cyber readiness
- unidentified sensitivity to cyber exposure

Implementation Guidance

Control Statement:

Scenario-based risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organisation's security programme.

Control Context:

Scenario-based risk assessments, including cyber wargames, test attacks on existing systems and processes targeting the hosted SWIFT ~~-related~~ infrastructure. Scenario-based risk assessments include technical and business driven exercises performed as part of institution risk management.

These assessments include the following threats: end-user impersonation, message tampering, message eavesdropping, third-party software weaknesses, compromising systems or Denial of Service (DoS) attacks affecting service availability. Results of the assessment and existing mitigations help identify areas of risks that may require future actions, risk mitigations or an update of the cyber-incident response plan.

Identified actions, mitigations, or updates must be reported and closed according to their criticality as per the Information Security Risk Management (ISRM) process.

Several ISRM frameworks exist and can be consulted[41] to define the user's proper ISRM and resources (such as CIS-Critical Security Controls). These frameworks can be used to start implementing a basic risk management process to be further enhanced to address user's specific risks.

Implementation Guidelines:

The implementation guidelines are common methods to apply the relevant control. The guidelines are a helpful way to begin an assessment, but should never be considered as an "audit checklist" as each user's implementation may vary. Therefore, in cases where some implementation guidelines elements are not present or partially covered, mitigations as well as particular environment specificities must be considered to properly assess the overall compliance adherence level (as per the suggested guidelines or as per the alternatives).

- A scenario-based risk assessment and planning activity is conducted to:
  - identify possible methods for adversaries to gain unauthorised access to local SWIFT infrastructure based upon observed adversary techniques or plausible adversary techniques inferred from adversaries' motivations and capabilities
  - analyse the effectiveness of existing prevention and detection controls to mitigate anticipated adversary techniques to gain unauthorised access to the environment
  - analyse the probability and impact of significant and plausible attack vectors given existing controls

[41] For example, on NIST, ENISA, COBRA or ISO sites or from a local or regulator's standard or controls set to the same level of rigour as industry guidance.

- analyse the effectiveness of existing response controls to limit impact of significant and plausible attack vectors given existing controls
- Identify the need for additional preventive or detective controls

- Assessment and planning activity is conducted at least annually, and updated through ongoing risk management activities, when significant technology changes occur, or when threat intelligence indicates relevant changes in an applicable adversary's capabilities or motivations.
- Current threat intelligence and observed or likely attacks (vectors, techniques, actors,) are used as the basis for scenarios.
- Each asset class (end-user devices, servers, network devices) is assessed against threats on a regular basis and when changes are introduced or when new threats are identified.

Appendix A: **Risk Driver Summary Matrix**

The matrix below is a summary of the risk drivers in this document, mapping the security controls to the documented risks they are intended to help mitigate.

SWIFT Security Controls **Risk Drivers**	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4A	2.5A	2.6	2.7	2.8A	2.9~~A~~	2.10	2.11A	3.1	4.1	4.2	5.1	5.2	5.3A	5.4	6.1	6.2	6.3	6.4	6.5A	7.1	7.2	7.3A	7.4A
Authentication token theft																					X										
Business conducted with an unauthorised counterparty														X		X															
Compromise of enterprise authentication system	X				X																										
Compromise of trusted back-up data										X																					
Compromise of user credentials	X				X																										
Credential replay	X				X														X												
Deletion of logs and forensic evidence		X																													
Excess attack surface								X							X																
Excess harm from deficient cyber readiness																												X			X
Excess privilege or access		X																		X											
Execution of malicious code																								X							
Exploitation of insecure system configuration								X							X																

SWIFT Security Controls / Risk Drivers	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4A	2.5A	2.6	2.7	2.8A	2.9A	2.10	2.11A	3.1	4.1	4.2	5.1	5.2	5.3A	5.4	6.1	6.2	6.3	6.4	6.5A	7.1	7.2	7.3A	7.4A
Exploitation of known security vulnerabilities							X					X												X								
Exposure to internet-based attacks	X			X	X																											
Exposure to sub-standard security practices													X																			
Increased security risk from improperly trained staff																														X		
Lack of traceability		X															X				X						X					
Loss of operational confidentiality											X																					
Loss of operational integrity											X																					
Loss of sensitive data confidentiality						X			X	X																						
Loss of sensitive data integrity						X			X																	X						
Password cracking, guessing, or other computational compromise																		X	X													
Password theft						X					X								X				X									
~~Segregation~~ Separation of duty violations																				X												
Unauthorised access	X		X		X	X														X												
Unauthorised physical access																	X															
Unauthorised system changes		X																							X							

SWIFT Security Controls / Risk Drivers	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4A	2.5A	2.6	2.7	2.8A	2.9A	2.10	2.11A	3.1	4.1	4.2	5.1	5.2	5.3A	5.4	6.1	6.2	6.3	6.4	6.5A	7.1	7.2	7.3A	7.4A
Unauthenticated system traffic						X			X																							
Uncontrolled proliferation of systems and data			X																													
Undetected anomalies or suspicious activity														X													X	X				
Unidentified sensitivity to cyber exposure																																X
Unknown security vulnerabilities or security misconfigurations																															X	
Untrustworthy staff or system operators																						X										

Appendix B: Secure Zone Reference Architectures

The following diagrams are for reference only, and describe one of many ways for the secure zones to be designed for each architecture (A1, A2, A3, A4, B).

Figure 10a: Secure Zones Example for Architecture A1
Interfaces within the user environment (on premises or in the Cloud)

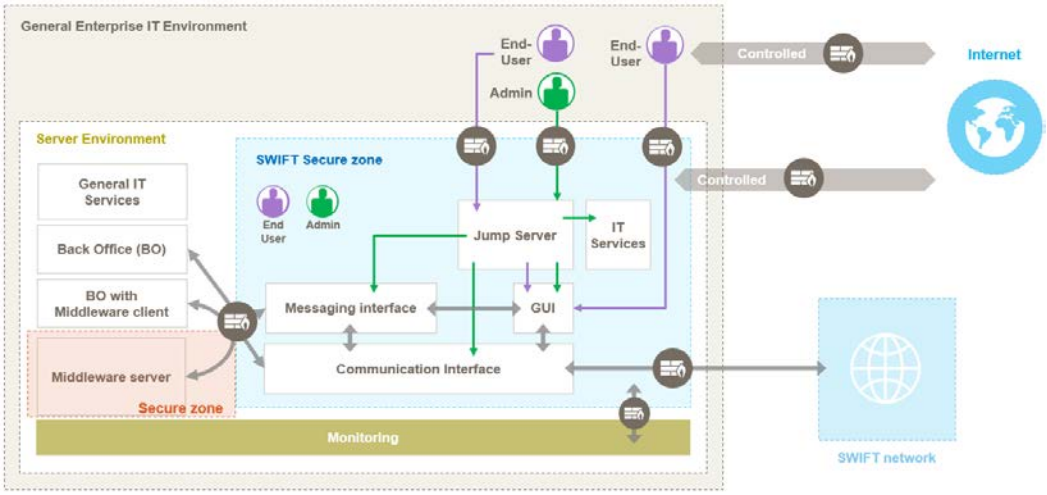


Figure 10b: Secure Zones Example for Architecture A1
Communication interface only within the user environment (on premises or in the Cloud)

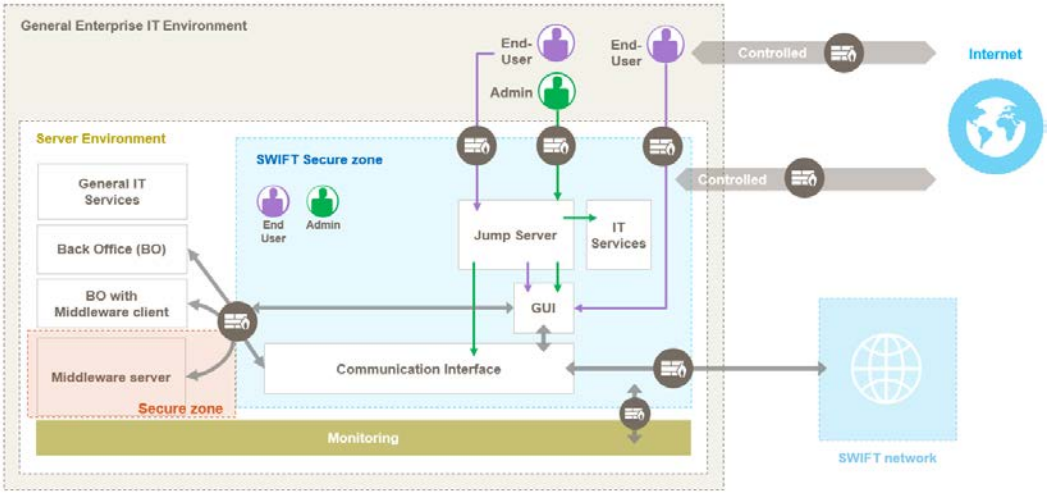


Figure 11: Secure Zone Example for Architecture A2
Messaging interface only within the user environment (on premises or in the Cloud)

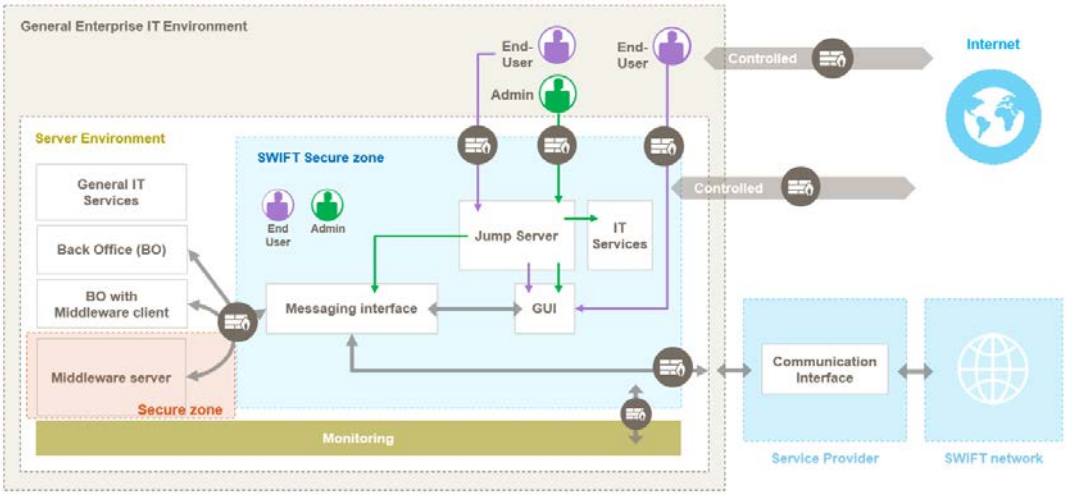


Figure 12a: Secure Zone Example for Architecture A3
SWIFT connector

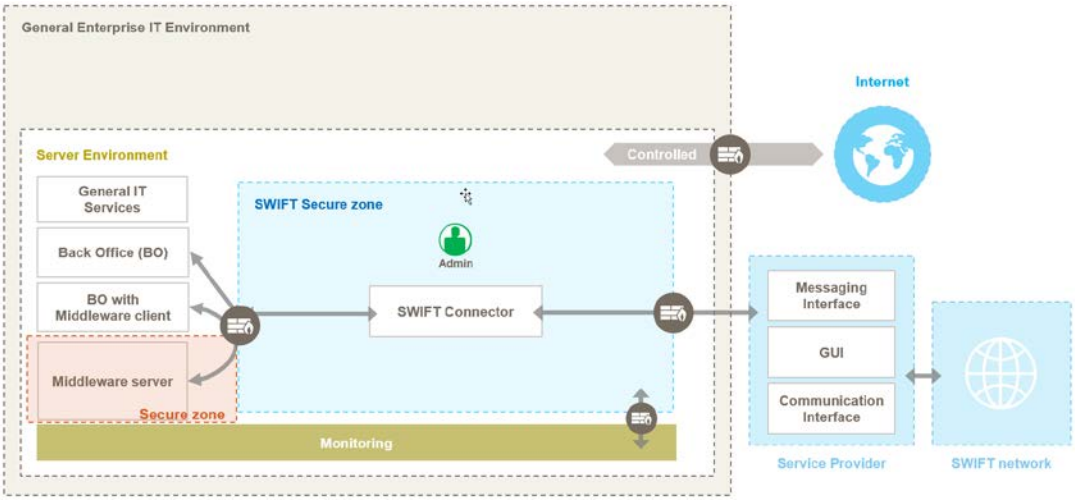


Figure 12b: Secure Zone Example for Architecture A4
Middleware server as Connector

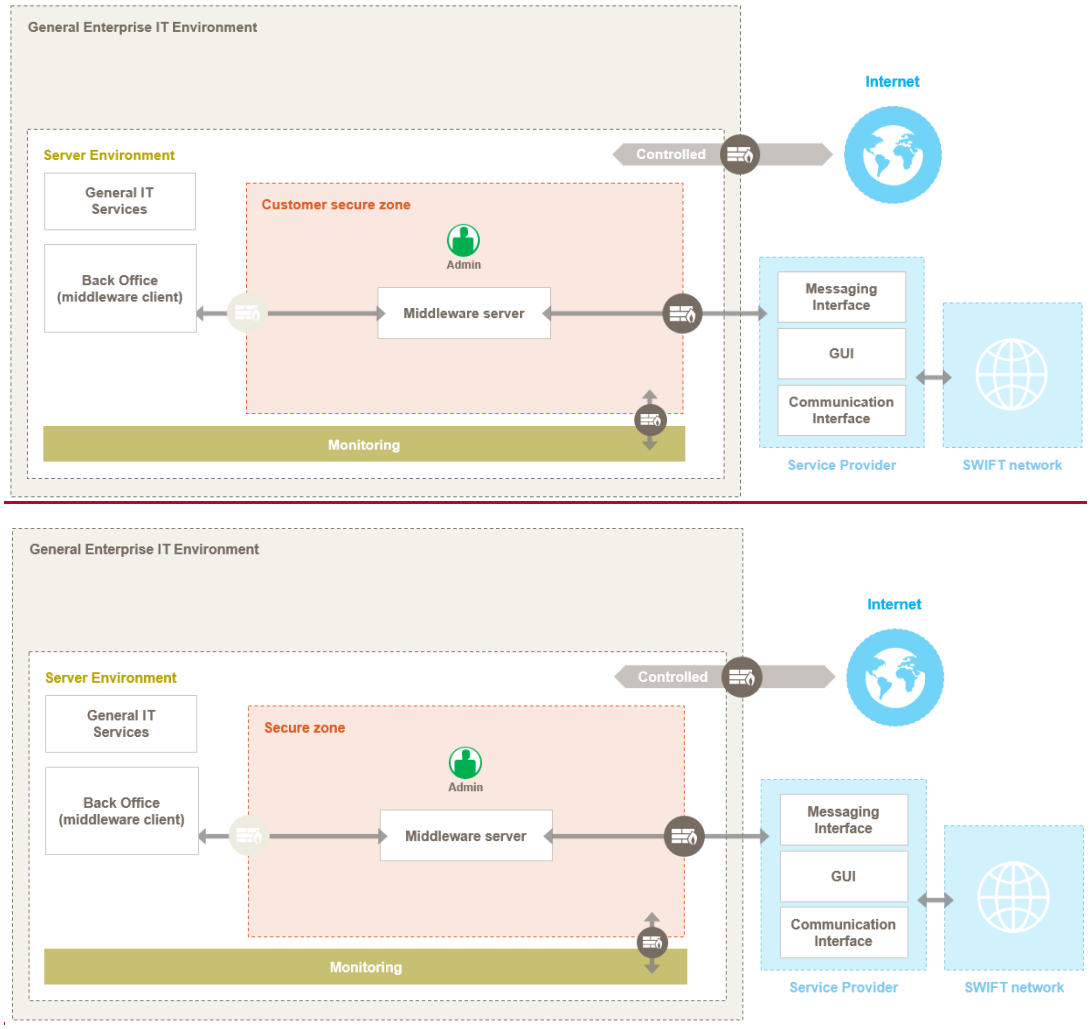


Figure 13a: Architecture B
No local footprint

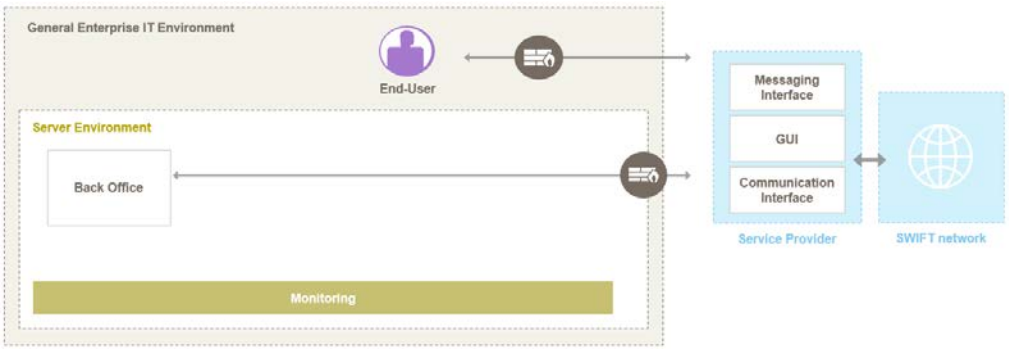
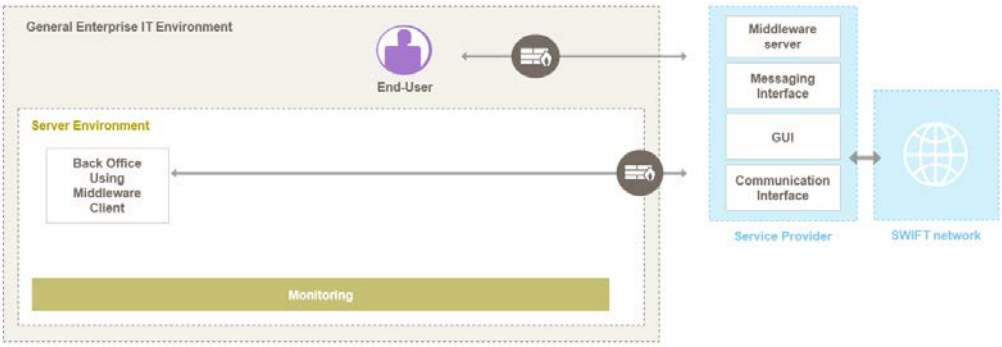


Figure 13b: Architecture B
No local footprint with middleware client



Appendix C: **Sample Threat Scenarios**

The following scenarios are examples to help users to understand the types of cyber threats that each security control is intended to help mitigate. These scenarios are non-exhaustive and provided for context and educational purposes only. The likelihood and impact of each scenario may differ significantly based on variables within the user environment.

1.1 SWIFT Environment Protection

- Attackers compromise credentials of the system administrator of the enterprise Active Directory, thereby granting the attackers access to all login credentials stored in the directory.
- Attackers compromise supporting IT infrastructure (for example, scanning server, patching server), located in the general IT environment. The objective is to steal system credentials and subsequently access the local SWIFT infrastructure.
- Attackers gain administrative access to an operator's PC, allowing the attacker to compromise the local account database and reuse the stored hashes to access other systems.
- ~~An operator clicks a malicious link in an e-mail, unknowingly downloading malware which compromises the local PC.~~

1.2 Operating System Privileged Account Control

- A system administrator using the root account in Linux performs unauthorised actions (for example, changing security configurations, causing an intentional system crash), which are not traceable to an individual operator.
- An operator with excess administrative privileges deletes logs and other forensic evidence to hide unauthorised actions.

1.3 Virtualisation Platform (also known as the hypervisor) Protection

- An attacker with access to the hypervisor could comprise the confidentiality, integrity and availability of virtual machines hosting SWIFT services.
- An attacker with access to the hypervisor provisioning function could create new virtual machines to support the attack. For example, they can create fake application services to cause users to divulge sensitive information or download malware.
- An attacker benefits of vulnerabilities or insecure configuration of the hypervisor to breach separation between hosted virtual machine domains to access virtual machines hosting SWIFT services.

1.4 Restriction of Internet Access

- Attackers compromise supporting IT infrastructure (for example, middleware server or virtualisation platform server), to steal system credentials and subsequently access the local SWIFT infrastructure.
- Attackers gain administrative access to an operator's PC, allowing the attacker to compromise the local account database and reuse the stored hashes to access other systems.
- An operator clicks a malicious link in an e-mail or web page, unknowingly downloading malware which compromises the local PC or server.

1.5A Customer Environment Protection

- Attackers compromise credentials of the system administrator of the enterprise Active Directory, thereby granting the attackers access to all login credentials stored in the directory.
- Attackers compromise supporting IT infrastructure (for example, scanning server, patching server), located in the general IT environment. The objective is to steal system credentials and subsequently access the customer infrastructure.
- Attackers gain administrative access to an operator's PC, allowing the attacker to compromise the local account database and reuse the stored hashes to access other systems.

2.1 Internal Data Flow Security

- An attacker with network access to the secure zone compromises the integrity of the transactions in transit between the messaging interface and communication interface.
- An attacker with network access to the secure zone is able to monitor unencrypted traffic between local SWIFT components and record confidential transactions.

2.2 Security Updates

- An attacker uses a known and unpatched vulnerability to gain access to a server hosting a SWIFT-related ~~application~~component.
- The operating system has aged beyond the vendor's support life-cycle window, resulting in persistent open vulnerabilities with no available remediation from the vendor.

2.3 System Hardening

- An attacker uses the default username and password to access the administration interface of a network firewall.
- An attacker uses a vulnerability associated with an unused network protocol (for example, telnet) to gain access to a SWIFT server.

2.4A Back Office Data Flow Security

- An attacker positioned on the used middleware server or between the back office and messaging interface injects unauthenticated transactions.
- An attacker creates a “person-in-the-middle” attack to change the beneficiary accounts of valid SWIFT transactions.
- An attacker positioned on the used middleware server or between the back office and messaging interface can monitor unencrypted traffic and record confidential transactions.

2.5A External Transmission Data Protection

- A data back-up location is compromised, and unencrypted SWIFT back-ups and credential hashes are accessed, providing the attacker with valuable information about SWIFT operators and typical activity within the local environment.
- Unencrypted back-ups of SWIFT servers are transmitted over an insecure network connection, resulting in an attacker gaining read-access to all recent messaging traffic records.

2.6 Operator Session Confidentiality and Integrity

- An operator leaves his desk and no timed screen lock-out is implemented, allowing an unauthorised person access to the operator's account and the SWIFT messaging interface.
- An attacker is able to perform surveillance on an unencrypted operator session, and learns from unencrypted information to plan a future attack.
- An attacker is able to perform surveillance on an unencrypted operator session, and steals credentials to create a fraudulent SWIFT transaction.
- An attacker intercepts a transaction sent between the browser and the web application, modifies the transaction content, and forwards it to the web application.
- An attacker is able to hijack an open session or bypass an authentication scheme due to unsafe settings to capture or create fraudulent SWIFT transactions.

2.7 Vulnerability Scanning

- A discoverable vulnerability is left unidentified and untreated, allowing an attacker to exploit the vulnerability to gain access to a SWIFT-related system~~server~~.

2.8A Critical Activity Outsourcing

- An outsourced provider does not properly separate SWIFT systems from other low-security systems, resulting in a virus spreading across environments and affecting the integrity of the SWIFT systems.
- An outsourced provider does not properly enforce access control, resulting in an unauthorised employee gaining access to the SWIFT messaging interface or other SWIFT-related components or systems.

2.9~~A~~ Transaction Business Controls

- Daily reconciliation is not performed, resulting in a fraudulent transaction going unnoticed until after the settlement date.
- Transactions are not limited to normal business hours, resulting in an unnoticed fraudulent transaction.

2.10 Application Hardening

- Default accounts or passwords can be used by attackers to gain unauthorised access to the application.
- Excessive privileges given to application users can be abused by attackers to perform unauthorised actions on the application.
- An attacker uses a vulnerability associated with an unused network protocol (for example, telnet) or functionality provided by unnecessary packages to gain access to a SWIFT server.

2.11A RMA Business Controls

- RMA relationships are not properly managed, resulting in the processing of a transaction from an unscreened~~vetted~~ or dormant counterparty.

3.1 Physical Security

- Poor log retention results in the inability to fully investigate which staff had physical access to the safe after a set of SWIFT HSM tokens were discovered to be missing.
- Weak data centre access control provides unauthorised staff with physical access to perform a physical-based attack on the SWIFT servers.

4.1 Password Policy

- A password policy is established, but not enforced, resulting in operators using weak passwords that are easily cracked during a cyber attack.
- A password of insufficient length allows the computation of a weak password hash, which an attacker steals from the PC's memory and allows him to recompute the original password.
- The same passwords are used by an administrator for systems inside and outside the secure zone, resulting in an adversary compromising the more exposed password and re-using this knowledge to gain access to the secure zone.

4.2 Multi-factor Authentication

- Multi-factor authentication is not implemented to access applications, resulting in an adversary using a stolen password to gain full access to the SWIFT messaging interface.
- Multi-factor authentication is not implemented to access the operating system of the messaging interface, resulting in an adversary using a stolen password to gain full administrative access to the system.

5.1 Logical Access Control

- “Least privilege” controls are not enforced, allowing an operator who only requires read-only access the ability to create and send SWIFT transactions.
- ~~Segregation~~ Separation of duty controls are not enforced, allowing a single operator to create and approve a SWIFT transaction, conflicting with the user's transaction approval policy.
- Account access is not promptly revoked, resulting in a recently transferred employee using their residual access to modify records on the SWIFT messaging interface.

5.2 Token Management

- Poor record keeping during assignment of connected and disconnected hardware or personal tokens results in the inability to revoke the correct tokens after staff members leave the organisation, allowing unknown and uncontrolled access.
- A token is left inserted in an operator's PC when not in use, allowing an attacker to use the token as an authentication credential as part of an attack.

5.3A Staff ~~Vetting~~ Screening Process

- A new employee with a previous judicial record for financial fraud is not screened~~vetted~~ before being granted operator access, resulting in an untrustworthy individual being placed in a position of trust.
- Current employees are not periodically ~~vetted~~screened, resulting in the organisation not having knowledge of an employee who has taken a part-time job with another financial institution and now has a significant conflict-of-interest.

5.4 Physical and Logical Password Storage

- A SWIFT operator stores his passwords on a piece of paper at his work area, allowing any staff member with physical access to the area to view the recorded password.
- A SWIFT application administrator stores his administrative passwords in a plain text file on his PC, thus allowing any PC system administrator access to the passwords.

6.1 Malware Protection

- Anti-malware software is not installed on the operator PC, resulting in a common malware executable compromising the PC after clicking a phishing e-mail.
- Anti-malware software on the SWIFT servers is not regularly updated, resulting in an otherwise detectable malicious executable causing harm to the servers.

6.2 Software Integrity

- An advanced attacker modifies the executable of the messaging interface and is not detected because software integrity checking has not been implemented.
- A malicious version of a software update is installed because the checksum was not verified at time of download.

6.3 Database Integrity

- A lack of database integrity checking allows targeted malware to delete database records while performing unauthorised transactions.
- A lack of database integrity checking allows an attacker to modify database records to hide evidence.
- A lack of database integrity checking allows a gap in sequential record numbering to remain undetected.

6.4 Logging and Monitoring

- Poor system logging results in the inability to trace malicious privileged commands to a specific individual during a cyber-incident investigation.
- Logs are collected, but not monitored, resulting in abnormal activity going undetected until significant financial harm has occurred.

6.5A Intrusion Detection

- A lack of intrusion detection capabilities results in unusual traffic outside normal business hours going undetected.
- A lack of intrusion detection capabilities results in unexpected protocol traffic for a given port going undetected.
- The intrusion detection system is not properly configured or monitored, resulting in discoverable intrusions remaining undetected because of the high number of false alarms.

7.1 Cyber Incident Response Plan

- An untested cyber-incident response plan results in a poor and uncoordinated response to a serious cyber intrusion, resulting in significant and avoidable financial harm.
- The failure to notify SWIFT during a cyber incident results in incomplete sharing of information, leading to similar cyber incidents at other institutions that could have been avoided.
- The inability to act upon cyber-threat intelligence leads to cyber intrusions that could have been avoided.

7.2 Security Training and Awareness

- SWIFT operators are not trained on best security practices, resulting in staff clicking malicious phishing e-mail links.

- SWIFT application administrators are not trained on security awareness related to their role and, as a result, do not detect or report suspicious activity on the SWIFT systems.
- SWIFT security officers lack knowledge related to their role and, as a result, do not properly assign privileges for operators, allowing the bypass of the ~~segregation~~ separation of duties principle.

7.3 Penetration Testing

- Penetration testing is not conducted in the SWIFT environment, and thus excessively permissive firewall rules are not discovered and corrected.
- Penetration testing is conducted by unqualified staff who are unable to simulate a typical financial industry attacker, which results in a false sense of security and low commitment to needed security improvements.

7.4A Scenario Risk Assessment

- Realistic risk scenarios are not tested within the organisation, resulting in an incorrect estimation of likelihood, impact, and overall cyber risk.
- Risk scenarios are tested without involvement of the business units and appropriate management, resulting in poor overall value of the activity and low commitment to needed security improvements.

Appendix D: **Glossary of Terms**

Term	Definition
Administrator	May refer to: Application Administrators - responsible for configuring, maintaining, and conducting privileged activities through an application interface. System Administrators – responsible for configuring, maintaining, and conducting other privileged activities through operating systems or other direct (non front-end) access.
Application account	Logons designated for an application. They are not meant to be used by a human, through a graphical user interface or interactive access. Application accounts have a password that is stored, retrieved, and used automatically by the application. An application account is typically used for integration purposes (for example, calling of API) or to support STP (straight-through-processing).
Asset class	A category of computing asset (for example, databases, servers, applications).
Back-office	The systems responsible for business logic, transaction generation, and other activities occurring before transmission into the local SWIFT infrastructure.
Communication interface	The software providing a link between the SWIFTNet network and Messaging Interface software or a back-office system. Communication interfaces provide centralised, automated, and high-throughput integration with different in-house financial applications and service-specific interfaces. Communication Interfaces are provided by SWIFT (for example, Alliance Gateway or Alliance Gateway Instant). Communication interfaces holding a SWIFT-compatible label can also be provided by third-party vendors.
Connector	A local software designed to facilitate communication with an external messaging or communication interface, both or to a service provider. When using a connector, interface components are usually offered by a service provider (for example, by a service bureau, hub infrastructure, or SWIFT).
Customer connector	File transfer solutions or middleware servers (such as IBM® MQ servers) used for external communication or connection are considered customer connectors as opposed to SWIFT-compatible products (such as communication and messaging interfaces or connector) delivered by SWIFT or related third-party vendors that are considered as SWIFT connector. In the future, an application integrating all functionalities to directly and independently connect to the SWIFT API Gateway to process transactions will also be considered as a customer (~~home-made~~in-house API) connector.
Common Vulnerability Scoring System (CVSS)	An open industry standard for assessing the severity of software vulnerabilities by assigning severity scores to these vulnerabilities, allowing for prioritisation of responses and resources in line with the threat.

Term	Definition
Cyber-security incident	Any malicious act or suspicious event that compromises, or was an attempt to compromise, a computing environment.
Data exchange layer	The transporting of data between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and a user back-office first hop, at application level, as seen from the SWIFT-related components.
Dedicated operator PC	An operator PC located in the secure zone and dedicated to interact with components of the secure zone.
Endpoint Detection and Response (EDR)	An emerging technology that addresses the need for continuous monitoring and a response to advanced threats by detecting suspicious activities and (traces of) other problems on hosts/endpoints.
Endpoint Protection Platform (EPP)	An emerging solution to address attack prevention. More frequently combines with EDR.
End User	An individual requiring interactive access to the application (for example, for business transactions, monitoring, and access control). This includes security officers and application administrators responsible for configuring and maintaining the application.
Four-Eyes principle	A security principle whereby two individuals must approve an action before it can be taken. This principle is also known as two-person rule.
General (enterprise) IT environment	The infrastructure used to support the broad organisation. This includes general IT services and general-purpose operator PCs.
General IT services	The supporting IT infrastructure, such as authentication services, asset management, databases, data storage, security services (for example, patching) and networking services (for example, DNS, NTP).
General-purpose operator PCs	An operator PC located in the general enterprise environment and used for daily business activities.
Graphical user interface (GUI)	A software that produces the graphical interface for a messaging interface, a communication interface or a connector~~a user~~ (for example, Alliance Web Platform, SWIFT Microgateway Front-End, and equivalent products).
Group Hub	A SWIFT user or a non-SWIFT user organisation connecting SWIFT users within its corporate group.
Hardware token	A USB token, smart card, or similar device.
Hosted database	The terminology used when a (user) database server or infrastructure (such as Oracle or the like) is used as opposed to an "embedded database" incorporated in the messaging interface itself.
Indicators of compromise (IOC)	Artefacts that can be observed on a network or operating system that might indicate system compromise.
Interactive login / session	The session model that indicates an exchange of data (for example, when a user enters data or a command and the system returns data).

Term	Definition
IT services	A set of components in support of business processes inside the secure zone, such as a release and patching deployment platform, Active Directory.
Jump server	A server used to provide access to the user secure zone from the user's corporate network (for example, Citrix or Remote Desktop).
Local Authentication (LAU)	The mechanism that provides integrity and authentication of files exchanged between applications. Local Authentication requires that the sending and receiving entity use the same key to compute a Local Authentication file signature.
Local SWIFT infrastructure	The collection of SWIFT-specific components within the user's production environment, including systems, applications, supporting hardware, tokens, and other authenticators. Also known as the SWIFT or customer sSecure zone.
Messaging interface	A software supporting the use of MT, MX, or ISO 20022 message standards through SWIFT FIN, InterAct, FileAct, and SWIFTNet Instant messaging services. The software provides the means for users to connect business applications to SWIFT messaging services and is typically connected directly to the communication interface. Messaging interfaces are provided by SWIFT (for example, Alliance Access or Alliance Messaging Hub). Messaging interfaces holding a SWIFT-compatible label can also be provided by third-party vendors.
Middleware	A software that enables two separate programs to interact or to exchange data with each other (for example, IBM® MQ, BizTalk, ConnectDirect).Usually composed of a Server and Clients running on the various interconnected systems (Client-Server model). In the case of peer-to-peer model without central server, connectivity can be considered as being direct between the systems (so not through middleware).
Middleware server	Local middleware systems implementations, such as IBM® MQ server (including MQ queues manager, MQ appliance or both), used for data exchange between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and a user back-office first hop as seen from the SWIFT-related components.
Multi-factor authentication	A method of user authentication where at least two different components are required to authenticate a user. The following authentication factors can be selected: • Knowledge factor (something the user knows), for example, a PIN or a password • Possession factor (something the user has), for example, an HSM token, a Digipass, mobile phone, or an RSA One Time Password device • Human factor (something the user is), for example, finger print or any other biometric
Network access control list (ACL)	The list of rules that are applied to port numbers or IP addresses for controlling traffic in and out. These lists are available on a network device.

Term	Definition
Network devices	Components used to assist in the management, routing, and security of the network (for example, routers, switches, firewalls).
Non-SWIFT footprint	A component deployed in user environment to link with SWIFT messaging services, SWIFT Transaction Management Platform, or a service provider, and that is not a messaging interface, a communication interface or a connector delivered by SWIFT or a related third-party vendor. Examples are File server solutions, middleware/MQ servers or customer (~~home-made~~in-house API) connector.
Operating system (OS) accounts	User accounts on a server or PC that are used for direct access to the operating system.
Operator	The term that collectively refers to both individual types below: End users – individuals requiring interactive access to the application (for example, for business transactions, monitoring, and access control). This includes security officers and application administrators responsible for configuring and maintaining the application. Operating System Administrators – responsible for configuring, maintaining, and conducting other privileged activities on the operating systems hosting the local SWIFT infrastructure.
Operator PC	The PC used by operators to conduct their duties.
Personal Identification Number (PIN)	A secret number that acts like a password preventing others from gaining unauthorised access to or using a token, mobile device or card.
Privileged account	An account on an operating system or application that gives elevated access beyond that of a typical user. Includes administrator accounts on operating systems, and security officer or application owner accounts on applications.
Reasonable comfort	A level of comfort that Management can obtain from internal or external subject matter experts (SME) when: - appropriate level of independence and objectivity of the SME is ensured, - fair validation by the SME of control design and implementation, confirms mitigation of risks as in the control objective, and - noted deviations do not materially impact the control's ability to mitigate the risk, or alternative controls compensate for such deviations. External assessments and certifications (such as against Systems and Organizations Controls (SOC) 2 or any~~the~~ industry standard~~s~~ identified in Appendix E like NIST or PCI-DSS) that cover CSCF controls, can~~may~~ give Management such reasonable comfort about the appropriateness of the controls as well as their operating effectiveness. The scope of this evaluation and the approach used for control evaluation in the context of such external assessments or certifications must be understood before relying on them either partially or fully.

Term	Definition
Relationship Management Application (RMA)	A filter that enables the user to limit the correspondents from which messages can be received and the type of messages which can be received. The use of the Relationship Management Application mechanism is mandatory for the FIN service. It is available on an optional basis for SCORE FileAct and Generic FileAct.
Remote access	The access to a computer from outside the local network. For example, from home or from another organisation's network.
Remote login	A login to a system initiated over a network connection rather than directly from the local PC.
Secure zone	A secure operational (sometimes also called production) zone on user premises separated from the general enterprise. The secure zone contains SWIFT-related systems (for example, messaging interface, communication interface, connectors), and, optionally, other protected systems.
Server Environment	A data centre or other secured physical location hosting servers.
Service bureau	A SWIFT user or non-user organisation that provides services to connect SWIFT users. The services offered by a service bureau typically include sharing, hosting, or operating SWIFT connectivity components, logins to the infrastructure, or managing sessions or security on behalf of SWIFT users. Service bureaux are subject to the Shared Infrastructure Programme.
Service provider	An organisation that usually provides services to SWIFT users regarding the day-to-day operation of the connection to SWIFT. The services offered typically include sharing, or operating SWIFT connectivity components, logins to the infrastructure, or managing sessions or security for SWIFT users. Such organisations include shared infrastructure providers (for example, service bureau, shared connectivity provider, SWIFT, Group Hub, intermediate actor).
Simple Object Access Protocol (SOAP)	An XML-based messaging protocol for exchanging information among computers.
Single user or safe mode	The protected mode of operation that limits the privileges of the user.
Software token	An authentication token in logical (software) form.
Staff	All individual people who collectively work for the same organisation (such as employees, agents, consultants and contractors).
SWIFT connector	A connector provided by SWIFT (for example, SWIFT Integration Layer (SIL) Direct Link, Alliance Lite2 AutoClient or Microgateway). A connector holding a SWIFT-compatible label provided by a related third-party vendor.
SWIFT footprint	A messaging interface, a communication interface or a connector provided by SWIFT or holding a SWIFT-compatible label and provided by a third-party vendor.
SWIFT-related application	SWIFT-related components or application exposed by a Service Provider

Term	Definition
SWIFT-related component	A software, product or element, usually deployed in a local infrastructure or secure zone, that supports SWIFT messaging and transactions services. Messaging and communication interfaces, SNL, SWIFT and customer connector, HSM, tokens, GUI as defined in the Scope of Security Controls section are examples of SWIFT-related components. Network devices protecting the secure zone can by extension also considered as SWIFT-related components but they are specifically mentioned when expected to be in-scope of a control.
SWIFT-related system	A host (physical box or virtual machine) running a SWIFT-related component
Thick client	A software program installed and executed on the local operator PC, rather than using a browser interface.
Third party	An entity independent of the SWIFT user or user's SWIFT connectivity provider. For example, an outsourced or external IT provider or cloud provider. By default, service bureaux and L2BA providers are considered service provider and not as third party, unless the SWIFT user specifically engages with them to host or to operate, or both, in full or in part the user's local SWIFT infrastructure (still owned by the user).
Transaction Authentication Number (TAN)	A type of single-use password generally used with a standard ID and password. Initially presented in a list or table.
(SWIFT) Transaction Management Platform	The future platform to be deployed centrally by SWIFT to offer complete transaction management in line with the strategy endorsed by the Board in March 2020.
Transport Layer Security (TLS)	A cryptographic protocol that secures communications by offering confidentiality, integrity and protection against replay attacks measures.
(SWIFT) User	An organisation that SWIFT has admitted under the Corporate Rules as a duly authorised user of SWIFT services and products. The eligibility criteria to become a SWIFT user are set out in the Corporate Rules.
User application accounts	User accounts established at the applications layer to grant access and permissions to the application (that is, not operating system accounts).

Appendix E: **Mapping to Industry Standards**

The table below maps the SWIFT security controls against three international security standard frameworks:

- National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce who developed a Cybersecurity Framework to help organisations to manage cyber-security risks.
- ISO 27002 ISO/IEC 27002 is an information security standard issued by the International Organisation for Standardization (ISO) and by the International Electrotechnical Commission (IEC).
- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations who work with and are associated with payment cards.

The following mapping table provides further details on how the SWIFT security controls relate to similar controls in those industry standards. If users are certified against any of these standards and under the condition the SWIFT infrastructure is in the scope of this certification, then the table indicates how the controls from these standards relate to the SWIFT security controls.

For other standards, SWIFT suggests using the informative references provided by NIST in the document Framework Core of their Cybersecurity Framework v1.1 (Appendix A) provided in the following table.

Important Note:

Meeting the requirements from these industry standards does not automatically imply full compliance with the SWIFT security control. Some aspects of the control might not be covered by the standard. It remains the ultimate responsibility of the user to assess whether and to which extent the compliance with one of these industry standards is suitable to assess the compliance with the SWIFT security controls.

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
1.1 SWIFT Environment Protection Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	**Access Control (PR.AC)** **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate	**Network security management (13.1)** **13.1.3**: Segregation in networks	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Applicable Subsection(s):** 1.3
1.2 Operating System Privileged Account Control Restrict and control the allocation and usage of administrator-level operating system accounts.	**Access Control (PR.AC)** **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties	**User access management (9.2)** **9.2.3:** Management of privileged access rights	**Requirement 8:** Identify and authenticate access to system components **Applicable Subsection(s):** 8.1, 8.5

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
1.3 Virtualisation Platform Protection Secure virtualisation platform (also referred to as the hypervisor) and virtual machines (VM) as physical servers.	Access Control (PR.AC) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) All subcategories	9 Access Control 10 Cryptography 11 Physical and environmental security 12 Operations Security 13 Communications Security 14 Systems acquisition, development and maintenance	**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters **Applicable Subsection(s):** 2.1 to 2.6
1.4 Restriction of Internet Access Control/Protect Internet access from operator PCs and other systems within the secure zone.	**Access Control (PR.AC)** **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate	**Network security management (13.1)** **13.1.3**: Segregation in networks	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Applicable Subsection(s):** 1.3
1.5 Customer Environment Protection Ensure the protection of the customer connectivity infrastructure from potentially compromised elements of the general IT environment and external environment.	**Access Control (PR.AC)** **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate	**Network security management (13.1)** **13.1.3**: Segregation in networks	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Applicable Subsection(s):** 1.3
2.1 Internal Data Flow Security Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related components.	**Data Security (PR.DS)** **PR.DS-2:** Data-in-transit is protected	**Information transfer (13.2)** **13.2.1:** Information transfer policies and procedures	**Requirement 4:** Encrypt transmission of cardholder data across open, public networks **Applicable Subsection(s):** 4.1
2.2 Security Updates Minimise the occurrence of known technical vulnerabilities on operator PCs and within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-12:** A vulnerability management plan is developed and implemented **RS.AN-5:** Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (for example, internal testing, security bulletins, or security researchers)	**Technical vulnerability management (12.6)** **12.6.1:** Management of technical vulnerabilities	**Requirement 6:** Develop and maintain secure systems and applications **Applicable Subsection(s):** 6.2

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
2.3 System Hardening Reduce the cyber-attack surface of SWIFT-related components by performing system hardening.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained.	**Security requirements of information systems (14.1)** **14.1.1:** Information security requirements analysis and specification	**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. **Applicable Subsection(s):** 2.2, 2.5
2.4A Back Office Data Flow Security Ensure the confidentiality, integrity, and mutual authenticity of data flows between SWIFT infrastructure components and the back-office first hop they connect to.	**Data Security (PR.DS)** **PR.DS-2:** Data-in-transit is protected.	**Information transfer (13.2)** **13.2.1:** Information transfer policies and procedures	**Requirement 4:** Encrypt transmission of cardholder data across open, public networks **Applicable Subsection(s):** 4.1
2.5A External Transmission Data Protection Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.	**Data Security (PR.DS)** **PR.DS-2:** Data-in-transit is protected.	**Information transfer (13.2)** **13.2.1:** Information transfer policies and procedures	**Requirement 3:** Protect stored cardholder data **Applicable Subsection(s):** 3.4
2.6 Operator Session Confidentiality and Integrity Protect the confidentiality and integrity of interactive operator sessions that connect to the local or remote (operated by a service provider) SWIFT infrastructure or service provider SWIFT-related applications.	**Data Security (PR.DS)** **PR.DS-2:** Data-in-transit is protected.	**System and application access control (9.4)** **9.4.2:** Secure logon procedures	**Requirement 8:** Identify and authenticate access to system components. **Applicable Subsection(s):** 8.1
2.7 Vulnerability Scanning Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.	**Continuous Monitoring (DE.CM)** **DE.CM-8:** Vulnerability scans are performed. **Risk Assessment (ID.RA)** **ID.RA-1:** Asset vulnerabilities are identified and documented. **RS.AN-5:** Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (for example, internal testing, security bulletins, or security researchers).	**Technical vulnerability management (12.6)** **12.6.1:** Management of technical vulnerabilities	**Requirement 11:** Regularly test security systems and processes **Applicable Subsection(s):** 11.2

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
2.8A Critical Activity Outsourcing Ensure the protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	**Business Environment (ID.BE)** **ID.BE-5:** Resilience requirements to support delivery of critical services are established. **Governance (ID.GV)** **ID.GV-2:** Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. **Supply Chain Risk Management (ID.SC)** ID.SC1 to ID.SC5	**Information security in supplier relationships (15.1)** **15.1.1:** Information security policy for supplier relationships	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.8
2.9 Transaction Business Controls Ensure outbound transactions activity within the expected bounds of normal business.	**Access Control (PR.AC)** **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties.	**Information transfer (13.2)** **13.2.2:** Agreements on information transfer	**Requirement 7**: Restrict access to cardholder data by business need to know **Applicable Subsection(s):** 7.1.4
2.10 Application Hardening Reduce the attack surface of SWIFT-related components by performing application hardening.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained.	**Security requirements of information systems (14.1)** **14.1.1:** Information security requirements analysis and specification	**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. **Applicable Subsection(s):** 2.1 to 2.5 **Requirement 6:** Develop and maintain secure systems and applications. **Applicable Subsection(s):** 6.2, 6.3, 6.4, 6.5, 6.7
2.11A RMA Business Controls Restrict transaction activity to validated and approved business counterparties.	**Access Control (PR.AC)** **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties.	**Information transfer (13.2)** **13.2.2:** Agreements on information transfer	**Requirement 7**: Restrict access to cardholder data by business need to know **Applicable Subsection(s):** 7.1.4

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
3.1 Physical Security Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.	**Access Control (PR.AC)** **PR.AC-2:** Physical access to assets is managed and protected.	**Secure areas (11.1)** **11.1.1:** Physical security perimeter **11.1.2:** Physical entry controls **11.1.3:** Securing offices, rooms and facilities **11.1.4:** Protecting against external and environmental threats **11.1.5:** Working in secure areas	**Requirement 9:** Restrict physical access to cardholder data **Applicable Subsection(s):** 9.1, 9.3, 9.5
4.1 Password Policy Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.	**Access Control (PR.AC)** **PR.AC-1:** Identities and credentials are managed for authorised devices and users.	**System and application access control (9.4)** **9.4.3:** Password management system	**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters. **Applicable Subsection(s):** 2.1 **Requirement 8:** Identify and authenticate access to system components **Applicable Subsection(s):** 8.2
4.2 Multi-factor Authentication Prevent that a compromise of a single authentication factor allows access into SWIFT-related systems or applications, by implementing multi-factor authentication.	**Access Control (PR.AC)** **PR.AC-1:** Identities and credentials are managed for authorized devices and users **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions. **PR.AC-7:** Users, devices, and other assets are authenticated (for example, single-factor, multifactor) commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organisational risks.	**System and application access control (9.4)** **9.4.2:** Secure log-on procedures	**Requirement 8:** Identify and authenticate access to system components. **Applicable Subsection(s):** 8.2, 8.3
5.1 Logical Access Control Enforce the security principles of need-to-know access, least privilege, and separation of duties for operator accounts.	**Access Control (PR.AC)** **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties.	**Business requirements of access control (9.1)** **9.1.1**: Access control policy	**Requirement 7:** Restrict access to cardholder data by business need to know **Applicable Subsection(s):** 7.1, 7.2

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
5.2 Token Management Ensure the proper management, tracking, and use of connected and disconnected hardware authentication or personal tokens (when tokens are used).	**Access Control (PR.AC)** **PR.AC-1:** Identities and credentials are managed for authorized devices and users.	**Responsibility for assets (8.1)** **8.1.2:** Ownership of assets	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.3
5.3A Staff Screening Process To the extent permitted and practicable, ensure the trustworthiness of staff operating the local SWIFT environment by performing regular staff screening.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-11:** Cybersecurity is included in human resources practices (for example, DE provisioning, personnel screening).	**Prior to employment (7.1)** **7.1.1:** Screening	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.7
5.4 Physical and Logical Password Storage Protect physically and logically the repository of recorded passwords.	**Access Control (PR.AC)** **PR.AC-1:** Identities and credentials are managed for authorised devices and users. **Data Security (PR.DS)** **PR.DS-1:** Data-at-rest is protected.	**System and application access control (9.4)** **9.4.3:** Password management system	**Requirement 8:** Identify and authenticate access to system components. **Applicable Subsection(s):** 8.2.1
6.1 Malware Protection Ensure that the local SWIFT infrastructure is protected against malware and act upon results.	**Security Continuous Monitoring (DE.CM)** **DE.CM-4:** Malicious code is detected.	**Protection from malware (12.2)** **12.2.1:** Controls against malware	**Requirement 5:** Protect all systems against malware and regularly update anti-virus software or programs. **Applicable Subsection(s):** 5.1, 5.2
6.2 Software Integrity Ensure the software integrity of the SWIFT-related components and act upon results.	**Data Security (PR.DS)** **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**Control of operational software (12.5)** **12.5.1:** Installation of software on operational systems **Security in development and support processes (14.2)** **14.2.4:** Restrictions on changes to software packages	**Requirement 11:** Regularly test security systems and processes. **Applicable Subsection(s):** 11.5

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
6.3 Database Integrity Ensure the integrity of the database records for the SWIFT messaging interface or the customer connector and act upon results.	**Data Security (PR.DS)** **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**Control of operational software(12.5)** **12.5.1:** Installation of software on operational systems **Security in development and support processes (14.2)** **14.2.4:** Restrictions on changes to software packages	**Requirement 11:** Regularly test security systems and processes. **Applicable Subsection(s):** 11.5
6.4 Logging and Monitoring Record security events and detect anomalous actions and operations within the local SWIFT environment.	**Protective Technology (PR.PT)** **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. **Anomalies and Events (DE.AE)** **DE.AE-2:** Detected events are analysed to understand attack targets and methods.	**Logging and monitoring (12.4)** **12.4.1:** Event logging	**Requirement 10:** Track and monitor all access to network resources and cardholder data. **Applicable Subsection(s):** 10.2, 10.6
6.5A Intrusion Detection Detect and prevent anomalous network activity into and within the local or remote SWIFT environment.	**Security Continuous Monitoring (DE.CM)** **DE.CM-1:** The network is monitored to detect potential cybersecurity events.	**Network security management (13.1)** **13.1.1:** Network controls	**Requirement 11:** Regularly test security systems and processes. **Applicable Subsection(s):** 11.4
7.1 Cyber Incident Response Planning Ensure a consistent and effective approach for the management of cyber incidents.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	**Management of information security incidents and improvements (16.1)** **16.1.1:** Responsibilities and procedures	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.10
7.2 Security Training and Awareness Ensure all staff are aware of and fulfil their security responsibilities by performing regular awareness activities, and maintain security knowledge of staff with privileged access.	**Awareness and Training (PR.AT)** **PR.AT-1:** All users are informed and trained.	**During employment (7.2)** **7.2.2:** Information security awareness, education and training	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.6

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
7.3A Penetration Testing Validate the operational security configuration and identify security gaps by performing penetration testing.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-12:** A vulnerability management plan is developed and implemented. **Risk Assessment (ID.RA)** **ID.RA-1:** Asset vulnerabilities are identified and documented. **RS.AN-5:** Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (for example, internal testing, security bulletins, or security researchers).	**Information security reviews (18.2)** **18.2.3:** Technical compliance review	**Requirement 11:** Regularly test security systems and processes. **Applicable Subsection(s):** 11.3
7.4A Scenario Risk Assessment Evaluate the risk and readiness of the organisation based on plausible cyber-attack scenarios.	**Risk Assessment (ID.RA)** **ID.RA-1:** Asset vulnerabilities are identified and documented. **ID.RA-3:** Threats, both internal and external, are identified and documented. **ID.RA-4:** Potential business impacts and likelihoods are identified **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. **ID.RA-6:** Risk responses are identified and prioritised.	**ISO 27001 Section 8.2**	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.2

Appendix F: Services and Components in scope per architecture type

To help users to identify the most important elements, the table below (version 2021_1.0) presents the services and components expected to be in scope and the usually related architecture type. It also presents, for informational purposes only, usual elements that are not in scope.

Note: This table will continuously be updated through the year. It is recommended to always use the latest version that can be found in the SWIFT Knowledge Base article 5024040 (CSP Components).

The following elements have to be considered when using the table:

- If multiple components are owned by a user and these components have different architecture types, then the user has to attest in KYC-SA against the most comprehensive architecture type using the decision tree, if needed.
- A component that is co-hosted with a component in scope is considered as in scope.
- All the components located in a secure zone have to be secured to the same level.
- <CTRL F> represents the most convenient way to locate a product.
- Components are listed alphabetically within each category.
- <effective date> refers to the date as of which a newly introduced component must be taken into account for the CSP Assessment. If empty, then it means it must already be taken into account.
- A, B - The Architecture type can be any "A" or "B".
- N/a - Not applicable.
- SWIFT recommends protecting components that are out of scope as if they were in scope.

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
	Interfaces and Related Applications	Communication Interface (for example, Alliance Gateway, Alliance Gateway Instant (AGI))	List of compatible communication interface: here Also includes API connectivity functionality based on AGI or Alliance Gateway	A1	
		Graphical user interface (GUI)	Products such as Alliance Web Platform (AWP), CREST GUI, SWIFT gpi GUI. SWIFT does not ensure compatibility of GUI provided by Vendors	A	
		IPLA - Alliance Access Integration Platform	Built on top of Alliance Access	A1/A2	
		IPLA - Connector For Sanctions Screening	Connector For Sanctions Screening is an IPLA component on Alliance Access	A1/A2	
		IPLA - gpi Connector	gpi Connector on IPLA is a vertical solution running as a set of components inside of Alliance Access IPLA infrastructure (runs within Alliance Access)	A1/A2	
		IPLA – TARGET2 Connector	TARGET2 Connector is an IPLA component on Alliance Access	A1/A2	
		IPLA – TARGET2 for Securities (T2S) Connector	T2S Connector is an IPLA component on Alliance Access	A1/A2	
		Messaging Interface (for example, Alliance Access, Alliance Messaging Hub (AMH))	List of compatible messaging interface: here Some back-offices can be considered as Messaging Interface (See KB article 5021823)	A1/A2	
		MQHA in relax/strict mode	Back-office using the MQHA in Relax and Strict mode are considered as Messaging Interface	A1/A2	
		RAHA in relax/strict mode	Back-office using the RAHA in Relax and Strict mode are considered as Messaging Interface	A1/A2	
		Relationship Management Application (RMA)	Can be stand-alone or integrated in the Alliance Access or AMH or vendor product – (see also here)	A1/A2	
		SwAP Proxy (gpi Connector) on AMH	gpi Connector on AMH is an AMH service running within AMH infrastructure (runs within AMH)	A1/A2	
		Remote File Handler (RFH) - FileAct	This component is used to transfer files and is installed in the messaging interface. Sometimes also referred by its executable name: SWFA Handler	A1/A2	
		Alliance Access used to connect to Alliance Remote Gateway (ARG)	This is an Alliance Access solution hosted on customer premises and accessing the Alliance Cloud solution at SWIFT.	A2	
		SWIFTNet Link (SNL)	Can be either included in the Communication Interface or stand-alone.	A1	
		SWIFT Translator (embedded)	when Embedded (that is integrated in the Messaging interface); **Out of Scope when stand-alone**	A1/A2	
	SWIFT Connector	Alliance Lite2 AutoClient	This is the File base solution interfacing with SWIFT Lite servers	A3	
		SWIFT Integration Layer (SIL) - Alliance Cloud	This is the SWIFT New Lite solution that replaces the AutoClient solution based on Direct Link.	A3	
		SWIFT Integration Layer (SIL) - Connector For Sanctions Screening	Connector For Sanctions Screening is a stand-alone component (discontinued as of January 2022)	A3	
		SWIFT Integration Layer (SIL) - gpi Connector (aka gpi Connector Stand alone)	gpi Connector on SIL is a vertical solution running as a set of components inside of SIL which is a stand-alone software (For example, gSRP or gCASE)	A3	
		SWIFT API Connector	Includes products such as Direct Link/SIL or SWIFT Microgateway.	A3	

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
		SWIFT Microgateway	Provides API connectivity functionality.	A3	
	Customer Connector	Customer API connector	Customer ~~home-made~~in-house API connector including API connectivity functionality, based on SWIFT API SDK specifications	A4	
		~~s~~FTP or FTPs solutions (servers)	Secure File transfer solutions used to facilitate communication with SWIFT-related components offered by a service provider.	A4	
		~~**[Advisory]**~~ Middleware/MQ Server	~~Advisory in scope in 2020.~~ Includes local middleware systems implementations, such as IBM® MQ server, used for data exchange/connectivity with a service provider~~between the SWIFT-related components (in the local SWIFT infrastructure or onsite at a service provider) and the user's backoffice.~~	A4	
	Hardware Components	Alliance Connect SRX VPN boxes or upcoming Alliance Connect~~the V~~virtual VPN instances (hosting systems or machines)	Only the CSP control 3.1 (Physical security) applies.	A, B	
		Connected and disconnected hardware authentication or personal tokens	Connected and disconnected hardware authentication or personal tokens used for SWIFT operations or secure zone access and PIN Entry Device (PED) used for HSM operations. **Includes the 3SKey personal tokens when used for SWIFT services (such as FIN, InterAct, FileAct in direct or through Alliance Cloud, Lite2 and in the future a messaging service or the Transaction Management Platform to be exposed by SWIFT).**	A, B	
		Hardware Security Module (HSM)	Typically combined with SWIFTNet Link SNL.	A1	
		Network devices protecting the secure zone(s)	Includes firewalls and routers.	A	
		Virtualisation Platform (Hypervisor)	Underlying layer on premises or with cloud providers hosting SWIFT-related virtual machines (VMs).	A, B	
	Operator PCs and Operators	Dedicated operator PC	An operator PC located in the secure zone and dedicated to interact with components of the secure zone.	A	
		General-purpose operator PC accessing the local or remote SWIFT infrastructure and the operators	An operator PC located in the general enterprise environment and used for daily business activities.	A, B	
		General-purpose operator PC used to access SWIFT Messaging Services hosted and operated at a service provider	General-purpose operator PC used to access SWIFT Messaging Services hosted and operated onsite at a service provider (such as a service bureau, an L2BA provider, an intermediate actor, or SWIFT) and when those PCs are used to submit or affect business transactions.	B	
		General-purpose operator PC used by Alliance Cloud or Lite 2 GUI Users	GUI users only do not have a connector.	B	
		General-purpose operator PC used by L2BA GUI Users	This covers PC that remotely connect to a front end application operated by a L2BA provider	B	
		General-purpose operator PC used by ESMIG user-to-application users	These are PCs connecting to the European Single Market Infrastructure Gateway (ESMIG) application over the SWIFT Network	B	

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
		General-purpose operator PC connecting to Sanctions Screening cloud solution	Sanction Screening uses central copy service. The solution is used to review the blocked payments in Sanctions Screening and decide wether they can be cancelled or released.	A, B	
		General-purpose operator PC connecting Transaction Screening cloud solution	Transactions Screening uses central copy service. The solution is used to review the blocked payments in Transaction Screening and decide whether they can be cancelled or released.	A, B	
		General-purpose operator PC connecting to WebAccess services	Using Web Platform/Alliance Gateway/SNL - over MV-SIPN	A1	
		"	Using Browser/Tokens - over MV-SIPN	B	
		"	Using Browser/Tokens - over the Internet	B	
		General-purpose operator PC accessing the gpi Tracker	Using Web Platform/Alliance Gateway/SNL - over MV-SIPN	A1	
		"	Using Browser/Tokens - over MV-SIPN	B	
		"	Using Browser/Tokens - over the Internet	B	
	MI products footprint used for Specific SWIFT Service	CRNet in Alliance Access	The CRNet component provides the user with a number of controls over the network connection from Alliance Access to the CRNet host application. It contains the underlying processes required for file transfer and interactive services.	A2	
		Euclid Connector Client (ECC) - for SWIFT traffic	Delivered by SWIFT to Euclid users and used for SWIFT traffic.	A1	
		Euclid Connector Host (ECH)	Delivered to EuroClear by SWIFT - only located at EuroClear premises.	Does not affect the architecture of the user	
		MI Channel for Continuous Link Settlement (CLS)	Market Infrastructure (MI) Channel is a messaging channel designed to enable customers to access large market infrastructures in an efficient manner. MI Channel relies on the SWIFTNet store-and-forward platform, and optimises the exchange of large amounts of data between the market infrastructure and their participants, while offering a simplified mode of operation and facilitating integration. MI Channel functionality is integrated within the existing communication Interface: SWIFTNet Link and Alliance Gateway.	A1	
		MI Channel for T2S	Software that manages the full communication stack for connecting to the T2S gateway in the SWIFT OPC specific to EuroClear.	A1	
		Minimum Footprint (MFP)	This solution is offered in two flavours: (i) embedded in SNL or (ii) as stand-alone, replacing the Alliance Access-Alliance Gateway-SWIFTNet Link, in both cases, they are in scope of the CSP.	A1	

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
		Transaction Delivery Agent (TDA)	The transaction delivery agent is an application, running on top of Alliance Gateway. It provides the transfer of messages between institutions. This transfer method offers a single and only one single guaranteed delivery of messages. The transaction delivery agent interface used to communicate with the applications of the institutions is based on the standard IBM WebSphere MQ messaging middleware.	A1	
	Others	Data Exchange Layer	The transport of data between the SWIFT-related components (in the local SWIFT infrastructure or onsite at a service provider) and a user back-office first hop as seen from the SWIFT-related components. Applicable controls: 2.4A, 6.4, 6.5A, 7.3A.	A, B	
		Jump Server giving access to the secure zone(s)	A server used to provide access to the user secure zone from the user's corporate network (for example, Citrix or Remote Desktop).	A	
		SOAP/API to connect from a back-office application to the Messaging Interface at a service provider	The SOAP connection method enables the exchange of MT, XML-based messages, and FileAct messages between Alliance Access and back-office applications.	B	
Not In scope		3SKey	A SWIFT personal identity solution based on PKI technology.3SKey tokens can be used with all banks to sign and approve transactions. 3SKey can be used on any electronic banking channel including in-house cash or treasury management systems, web banking, local and proprietary networks and SWIFT. You can use it to sign electronically banking instructions or connect securely to your banking application. **Note that 3Key personal tokens used for SWIFT services are in scope (refer to Hardware Components category above)**	N/a	
		Australia New Payments Platform (AU-NPP) and Go Local India (GLI) users	Not considered as SWIFT users.	N/a	
		The back office	The systems responsible for business logic, transaction generation, and other activities occurring before transmission into the local SWIFT infrastructure. For example, back-office implementations such as SAP and General Ledger are out of scope.	N/a	
		Business Intelligence systems (for example, SWIFT Scope)	Although globally out of scope, **SWIFT recommends the Business Intelligence systems defined as destination for transmitted sensitive data to be included in the control '2.5A External Transmission Data Protection'.**	N/a	
		Connections to the SWIFT network supplied by SWIFT Network Partners	This includes the (i) Connection to the four SWIFT providers (BT Global Services, Orange Business Services, AT&T and Colt) behind the VPN Boxes and (ii) Internet connections.	N/a	
		Euclid Client Connector (ECC) - Not for SWIFT traffic	Delivered by SWIFT. SWIFT provides the connector but BT Radianz provides the network connectivity.	N/a	
		Euclid PC	Delivered by EuroClear to EuroClear customers.	N/a	
		Euclid Server	Delivered by EuroClear.	N/a	

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
		General Enterprise IT environment	The general IT infrastructure used to support the general organisation (for example, general-purpose PCs, mail server, directory services)	N/a	
		General-purpose operator PC accessing the gpi Basic Tracker	When using swift.com accounts only for Basic Tracker functionalities. It is not used for Stop and Recall.	N/a	
		MQ Client on back-office system	This is a software component that enables an application running on a system to issue calls to a queue manager (MQ Server) running on another system. The output from the call is sent back to the MQ client, which passes it to the application.	N/a	
		MQHA in Basic mode	Back-office application using the MQHA in **Basic** mode are considered as back-office.	N/a	
		RAHA in Basic mode	Back-office application using the RAHA in **Basic** mode are considered as back-office.	N/a	
		Payment Gateway/Domestic Messaging Channel (PAG/DMC) for AU-NPP	Not considered as SWIFT users.	N/a	
		Payment Control Service (PCS)	A solution used to identify and prevent fraudulent or out-of-policy payment instructions for sent payments. **SWIFT recommends the tokens associated to this service to be covered in the control 5.2 Token Management.**	N/a	
		Pre-validation for SWIFT gpi	The gpi pre-validation detects payment problems before payments are sent for execution. There is consequently no specific risk in terms of CSP. The gpi pre-validation uses the SWIFT API Gateway. It must authenticate with the SWIFT API platform, which can be facilitated by using dedicated technology, such as the connector for SWIFT gpi. It can be based on SDK, SDK + gpi stand-alone connector, or by using interfaces and an embedded gpi connector.	N/a	
		Pre-validation gpi webserver	Used for queries only and does not impact the integrity of the transactions.	N/a	
		Sanctions Screening using central copy service - cloud solution	This solution is used to screen transactions for sanctions compliance, and review the alerted blocked payments in Sanctions Screening and then they can be cancelled or released. Therefore, end users do not initiate or modify payments in Sanctions Screening. If a payment is released then it means that it has passed all transaction controls in the messaging interface (for example, Four-Eyes, Six-Eyes) and this is just an additional check for compliance purposes with those regulatory lists (UN, States, and other lists). End users use WebAccess~~the GUI~~ to access the Sanctions Screening GUI in the cloud. **SWIFT recommends that the tokens associated to this service be covered in the control 5.2 Token Management.**	N/a	
		SWIFT Scope	A business intelligence solution providing full and immediate visibility on an organisation's daily cash reporting.	N/a	

In Scope/Not in CSP Scope	Category	Component Name (alphabetical within each category)	Description/Remark	Likely CSP Architecture Type(s)	Effective date
		SWIFT SDK on back-office application (when relying on SWIFT footprint or customer connector)	Not in scope when relying on other SWIFT-related ~~applications or~~ components to connect to SWIFT Messaging/Transaction Services (using a communication interface or a SWIFT (API) connector as SWIFT footprint).	N/a	
		SWIFT Translator (stand-alone)	Out of scope when stand-alone. **In-scope when embedded in the Messaging Interface.**	N/a	
		Transaction Screening using central copy service - cloud solution	This solution is used to screen transactions for sanctions compliance, and review the alerted blocked payments in Transaction Screening and then they can be cancelled or released. Therefore, end users do not initiate or modify payments in Tansaction Screening. If a payment is released then it means that it has passed all transaction controls in the messaging interface (for example, Four-Eyes, Six-Eyes) and this is just an additional check for compliance purposes with those regulatory lists (UN, States, and other lists). End users use WebAccess to access the Transaction Screening GUI in the cloud. **SWIFT recommends that the tokens associated to this service be covered in the control 5.2 Token Management.**	N/a	
		WebAccess servers at provider side	A server hosted on a service provider's premises and supporting a web-based service.	N/a	

Appendix G: Shared Responsibilities in an IaaS Cloud Model

Users engaging with third parties (such as an external IT provider or cloud provider) or service providers (such as a service bureau or a Lite2 Business Application provider) in order to host or operate their own SWIFT infrastructure in full or in part, must get reasonable comfort from those third parties or service providers that the related activities are protected in line with CSCF security controls. As such, third parties can rely on their compliance programme that usually builds on SOC 2, PCI-DSS or NIST certifications or assurance to answer users engaging with them and map the CSCF security controls. The user remains responsible and accountable for the attestation they need to fill taking into account the deployed controls and those deployed by the involved third parties and service providers.

Not all outsourcing models can be covered here. Therefore, to illustrate and trigger users' choice when considering the outsourcing model, the table below presents the typical sharing of responsibilities when an Infrastructure as a Service (IaaS) model in the cloud, similar to the Digital Connectivity Initiative* one (when available), is selected.

* In the Digital Connectivity Initiative, the user subscribes to a virtualised environment set up by selected cloud providers (CP) on the cloud infrastructure. The user remains responsible for the deployment, management of the various stacks (systems and applications) in the subscribed environment and, therefore, of the related controls. The ~~HSM and the~~ VPN can be physically hosted, or later virtualised, in the cloud provider infrastructure. The HSM has to be physically hosted (on-premises or in a co-location data centre). If the majority of the systems or components of an architecture A1 are hosted with the cloud provider, then the user still has on premises some equipment, as a minimum the operator PCs, that they need to protect.

Control	User	CP	Relevance for the Cloud Provider (CP)
1.1 SWIFT environment protection.	X	X	Segregated virtualised user environment [mainly through 1.1.c by design, network & operations]
1.2 OS privileged accounts control.	X	X	On the virtualisation infrastructure/environment set up by the CP
1.3 Virtualisation platform protection	X if used	X	Supporting the virtualisation infrastructure/environment set up by the CP.
1.4 Restriction of internet access.	X	X	Protection of the virtualisation infrastructure/environment set up by the CP
2.1 Internal data flow security	X		
2.2 Security updates.	X	X	On the virtualisation infrastructure/environment (and admin desktop)
2.3 System hardening	X	X	On the virtualisation infrastructure/environment (and admin desktop)
2.4A Back Office data flow security.	X	X	Secure exchange with the virtualisation infrastructure/environment and subscription of the user
2.5A External transmission data protection.	X	X	Virtualisation infrastructure/environment back-ups and transfers (between virtual stacks). Protect data storage (ideally through encryption – data at rest or environment/subscription)
2.6 Operator session confidentiality, integrity.	X	X	Limited to virtualisation infrastructure/environment and dedicated operator PCs
2.7 Vulnerability scanning	X	X	On the virtualisation infrastructure/environment
2.8A Critical activity outsourcing	X		To be considered by user depending on outsourced model (HSM) – VPN is managed by SWIFT Potential access to data to be covered in contract (if possible through virtualised environment)
2.9A Transaction business controls	X		
2.10 Application hardening	X		
2.11A RMA business controls	X		

Control	User	CP	Relevance for the Cloud Provider (CP)
3.1 Physical security	X	X	Of the virtualisation infrastructure/environment.
4.1 Password policy	X	X	On the virtualisation infrastructure/environment and the subscription set up for the user
4.2 Multi-factor authentication.	X	X	Support secure access to the virtualisation infrastructure/environment set up for the user
5.1 Logical access control	X	X	On the virtualisation infrastructure/environment and the subscription set up for the user
5.2 Token management.	X	X	Solution dependent (HSM or others used by CP to access the virtualised infrastructure)
5.3A Personnel vetting process	X	X	For operators of the virtualisation infrastructure/environment and subscription set up for the user
5.4 Physical and logical password storage	X	X	For the virtualisation infrastructure/environment, subscription and solution dependent (HSM or ?)
6.1 Malware protection.	X	X	Solution dependent on the virtualisation infrastructure/environment and operator PCs
6.2 Software integrity	X		
6.3 Database integrity	X		
6.4 Logging and monitoring	X	X	On the virtualisation infrastructure/environment and the subscription set up for the user
6.5A Intrusion detection	X	X	On the virtualisation infrastructure/environment and the subscription set up for the user (RACI)
7.1 Cyber incident response planning.	X	X	To be incorporated in customer incident response plan
7.2 Security training and awareness.	X	X	For operators of the virtualisation infrastructure/environment and subscription set up for the user
7.3A Penetration testing	X	X	On the virtualisation infrastructure/environment supporting the subscription set up for the user.
7.4A Scenario risk assessment	X	X	On the virtualisation infrastructure/environment supporting the subscription set up for the user.

Legal Notices

Copyright

SWIFT © 2021. All rights reserved.

~~**Restricted Distribution**~~

~~Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.~~

Confidentiality

This publication contains SWIFT or third party confidential information. Do not disclose this publication outside your organisation without SWIFT's prior written consent. You may however share this publication on a need-to-know basis with third parties that support you in connection with the SWIFT Customer Security Programme initiatives provided (i) you inform the recipient of the confidential nature of the information and (ii) you ensure that it is bound by no less stringent obligations of confidentiality.

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of SWIFT documentation is the only official and binding version.

Trademarks

SWIFT is the trade name of S.W.I.F.T. SC. The following are registered trademarks of SWIFT: 3SKey, Innotribe, MyStandards, Sibos, SWIFT, SWIFTNet, SWIFT Institute, the Standards Forum logo, the SWIFT logo, SWIFT gpi with logo, the SWIFT gpi logo, and UETR. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.