SWIFT Customer Security Controls Framework v2020

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 good practices that SWIFT recommends each user implement in their operating environment.

04 July 2019

Table of Contents

Executive Summary

Cyber attacks are becoming increasingly sophisticated in the financial community. The persistence of such threats underlines the importance of remaining vigilant and proactive over the long term. While customers are responsible for protecting their own environments and access to SWIFT, the Customer Security Programme (CSP) has been introduced to support customers in the fight against cyber fraud. The CSP establishes a common set of security controls designed to help customers to secure their local environments and to foster a more secure financial ecosystem.

The SWIFT Customer Security Controls Framework describes a set of mandatory and advisory security controls for SWIFT users. Mandatory security controls establish a security baseline for the entire community, and must be implemented by all users on their local SWIFT infrastructure. SWIFT has chosen to prioritise these mandatory controls to set a realistic goal for near-term, tangible security gain and risk reduction. Advisory controls are based on good practice that SWIFT recommends users to implement. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The controls have been developed based on SWIFT's analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. The control definitions are also intended to be in line with existing information security industry standards.

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

Given the evolving nature of cyber threats, it is the intention to regularly assess the controls, and to refine and expand them by publishing a new version of this document. Consequently, please ensure that you always use the latest available version of this document located in the Knowledge Centre.

To support adoption of the controls, SWIFT has developed a process that requires users to self-attest compliance against the mandatory and, optionally, the advisory security controls. Users are asked to submit a self-attestation into the KYC Registry Security Attestation application (KYC-SA). By the end of each year, each user must self-attest compliance against the mandatory and, optionally, the advisory security controls as documented in the CSCF in effect at that time. A new version of the CSCF is typically published in early July listing the mandatory and advisory controls to self-attest against as from July of the following year when implemented in the KYC-SA. To illustrate, users must self-attest between July and December 2020 against the security controls listed in the CSCF v2020 published mid-2019.

Each user retains control over their own data and is able to grant access to allow their counterparties to view their self-attestation data. This fosters transparency, and creates peer-driven momentum to improve security by allowing other users on the network to apply risk-based decision-making concerning their business relationships. For more information about the attestation and reporting process, see the latest version of the *SWIFT Customer Security Controls Policy* found in the Knowledge Centre.

The CSP is designed to be a collaborative effort between SWIFT and its users to strengthen the overall security of the financial ecosystem. All users must therefore read the controls set out in this document carefully, and prepare for implementation within their own organisation.

Overview of changes

The SWIFT Customer Security Controls Framework version 2020 promotes two advisory controls from the previous release to mandatory security controls (1.3 and 2.10) and introduces two new advisory controls (1.4A and 2.11A). The scope is also, advisory to start with, extended to the middleware servers. It also provides some additional guidance and clarifies, where applicable, implementation guidelines or alternative implementations.

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.

Control or section	Change
Raise the bar - advisory controls promoted to mandatory	
1.3 Virtualisation Platform Protection	Mandate protection of the Virtualisation Platform (underlying layer) hosting SWIFT related Virtual Machines. Virtualisation Platform added as in-scope element of relevant subsequent controls to prevent virtualisation sprawl
2.10 Application Hardening	Mandate secure configuration of the interfaces to reduce risks of unexpected application access, functionalities misuse or segregation of duties bypass
Raise the bar - new advisory controls or scope extension	
1.4A Restriction of Internet Access	Centralise the guidance related to internet access (and removal from 1.1 when turned Mandatory)
Scope of Security Controls 2.4A Back Office Data Flow Security	Scope extension for some controls (advisory when middleware/MQ servers are used)
2.11A RMA Business Control	Split Transaction and RMA business controls from the control 2.9A (different time horizon)
Additional guidance	
5.2 Tokens Management	Clarification on a) tokens reassignment or disposal b) Hardware Security Module (HSM) PIN Entry Device (PED) keys usage control
Alignment to reality - valid alternative implementation	
6.5A Intrusion Detection	Refer to both NIDS and HIDS and add potential alternative implementation
Clarification to existing controls	
Scope of Security Controls	Remind that a) self-attestation covers live, back-up and disaster recovery environment b) test systems are segregated from production systems or maintained as production ones.
Architecture Types	Architecture A1 also includes setups whereby the user only owns a communication interface, not necessarily both interfaces Scope extension to middleware/MQ servers might turn some B architecture to become A3
Security Controls Compliance	Additional wording to support the enforced assessment and to stress that implementation guidelines are not audit

Control or section	Change
	check lists
Security Controls Summary	Visualisation of components where the controls apply
Expectations on General Operator PCs	Some controls are expected on Operator PCs irrespective of Jump Server usage i.e.: 1.4A Internet Access; 2.2 Security Updates; 2.3 System Hardening; 2.6 Session Protection; 3.1 Remote Workers; 4.1 Password Policy; 6.1 Malware Protection
1.1 SWIFT Environment Protection	Reliance on some elements located in a (non-SWIFT) secure zone
2.1 Internal Data Flow Security 2.6 Operator Session, Confidentiality and Integrity	Improved split between application flows (2.1) and human/interactive flows (2.6)
2.5A External Transmission Data Protection	Clarification for better split with 2.4A and focus on result of (i) on backups, archiving, (ii) data extraction as per operational process
2.8A Critical Activity Outsourcing	Clarification on third party usage
5.3A Personnel Vetting Process	Emphasis on the link with applicable laws and regulations
6.1 Malware Protection	Clarification regarding the scope and full on-demand scans
7.2 Security Training Awareness	Reference to spear phishing
7.3A Penetration Testing	Scope clarification and reference to the CSP FAQ

Framework Objectives and Principles

Objectives and Principles

The security controls are based upon 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:

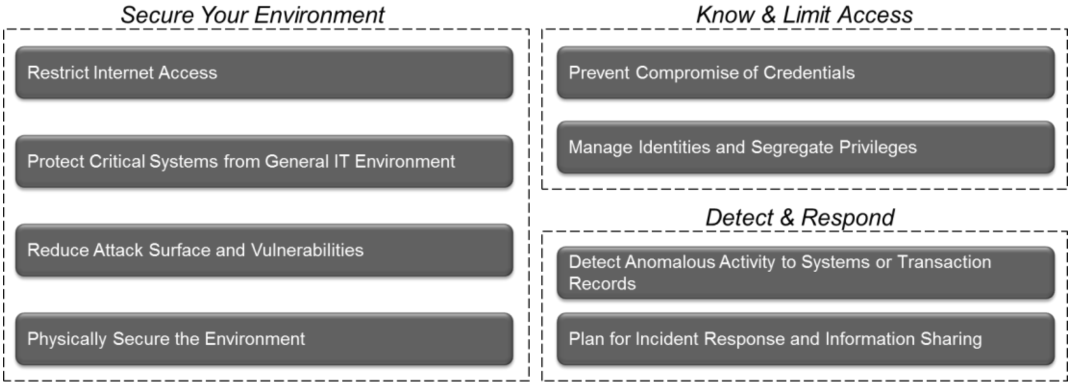
Secure Your Environment
Restrict Internet Access
Protect Critical Systems from General IT Environment
Reduce Attack Surface and Vulnerabilities
Physically Secure the Environment
Know & Limit Access
Prevent Compromise of Credentials
Manage Identities and Segregate Privileges
Detect & Respond
Detect Anomalous Activity to Systems or Transaction Records
Plan for Incident Response and Information Sharing

Figure 1: Framework Objectives and Principles

The 31 security controls (21 mandatory and 10 advisory controls) detailed in this document underpin these objectives and principles. The controls are intended to help mitigate specific cybersecurity 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:

- Unauthorised sending or modification of financial transactions
- Processing of altered or unauthorised SWIFT inbound (i.e. 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:

- 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-off or one-time activity, nor as exhaustive or all-inclusive. Users should rather incorporate SWIFT's controls into an ongoing cybersecurity governance and risk programme within their organisation that considers sound judgment 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. SWIFT has also published a guiding document to assist financial institutions in assessing their counterparty cybersecurity risk and incorporating this into their risk management framework.

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

In addition, users should have the right level of accountability and oversight for their cyber risk management activities. Typically, 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 security controls in this document are scoped to encompass a defined set of components in the user's local environment (see Figure 2).

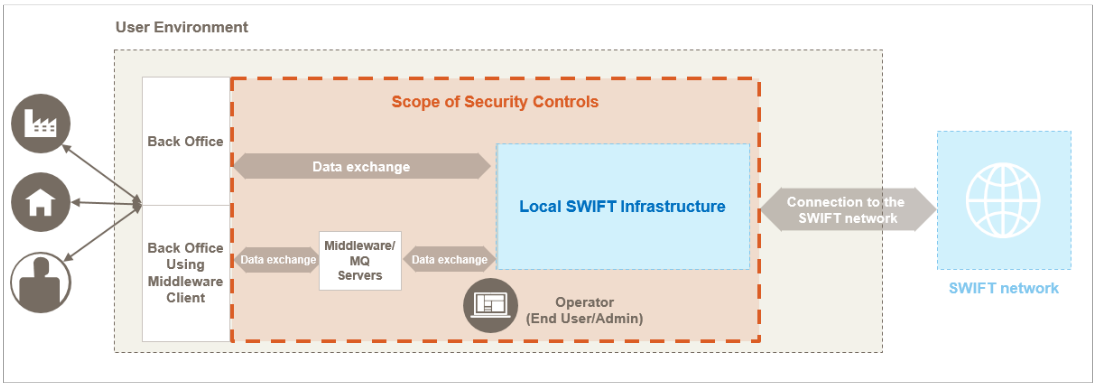
User Environment
Back Office
Back Office Using Middleware Client
Scope of Security Controls
Data exchange
Local SWIFT Infrastructure
Data exchange
Middleware/ MQ Servers
Data exchange
Operator (End User/Admin)
Connection to the SWIFT network
SWIFT network

Figure 2: Scope of Security Controls

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

- **Local SWIFT infrastructure –** The collection of SWIFT-specific components managed by or for users, including applications, network components, tokens and other removable media, and supporting hardware. Examples of local SWIFT infrastructure set-up and components, depending on the user architecture type, are:
  - **Secure Zone -** segmented zone separating SWIFT-related systems from the wider enterprise (further detailed in Control 1.1). This zone may expand beyond the local SWIFT infrastructure and may include non-SWIFT systems.
  - **Messaging Interface -** Messaging Interface software supporting the use of 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. Messaging interfaces are provided by SWIFT (for example, Alliance Access and Alliance Messaging Hub or Alliance Messaging Hub Instant) and by certified third-party vendors.
  - **Communication Interface -** Communication Interface software providing a link between the SWIFTNet network and Messaging Interface software. 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) and by certified third-party vendors.
  - **Connector -** Connectors are local software designed to facilitate communication with a messaging or communication interface, or both. When using a connector, interface components are offered by a service provider (for example, by a service bureau, hub infrastructure, or SWIFT). Alliance Lite2 AutoClient, DirectLink, file transfer solutions, and equivalent products are considered connector solutions. Similarly, local middleware systems implementations, such as IBM® MQ server, used to communicate with SWIFT-related components offered by a service provider are also considered connector solutions.
  - **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 as part of the Communication Interface scope.
  - SWIFT Hardware Security Modules, connected tokens and smart-cards.
  - Firewalls, routers, etc. within or surrounding the SWIFT infrastructure (dedicated or shared).

  - **Graphical user interface (GUI)** - Software that produces the graphical interface for a user (for example, Alliance Web Platform Server-Embedded and equivalent products).
- **Operators** - Operators are individual end users and administrators who directly interact with the local SWIFT Infrastructure at the application or OS level.
- **Operator PCs -** These are the end user or administrators' computing device (typically a desktop or laptop) used to conduct their duties (use, operate or maintain) the local SWIFT infrastructure.
  - This component may refer to a jump server, and not the operator's personal computing device, if such architecture is implemented.
  - The terms, "general purpose Operator PC" and "dedicated Operator PC" are defined as:

    A ***general purpose Operator PC*** is located in the general enterprise IT environment and used for daily business activities including accessing the local SWIFT infrastructure.

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

    When used on its own, ***Operator PC*** includes both general purpose and dedicated Operators PCs.
- **Data exchange layer –** The transport of data between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office first hop as seen from the SWIFT-related components.
- **Middleware Server –** Local middleware systems implementations, such as IBM® MQ server, used for data exchange between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office.

The following components are out of scope:

- **User 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.
- **General Enterprise IT environment -** The general IT infrastructure used to support the broad organisation (for example, general purpose PCs, mail server, directory services, etc.).

Connections to the SWIFT network supplied by SWIFT Network Partners, Internet connection to the SWIFT network, and Alliance Connect VPN boxes remotely managed by SWIFT are also out of scope. However, Alliance Connect VPN boxes are expected to be in an environment with appropriate physical controls in line with security control 3.1.

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

Note: Users must self-attest for all in-scope components in their local live, back-up and disaster recovery environment, taking into account their specific architecture.

As such, test systems are preferably fully segregated from production systems (incl. separate HSMs) and configured to only support test traffic (for example, by only using lite certificates and only configuring test logical terminals). If not fully segregated, 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.

Architecture Types

Each user must identify which of the four reference architecture types (Figures 3-6) most closely resembles their own architecture deployment to determine which components are in scope. Depending on the architecture type, some security controls may or may not apply.

The four reference architectures are as follows where component or license 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.

  The below picture depicts the case where both the messaging interface and communication interface are owned by and within the user environment.

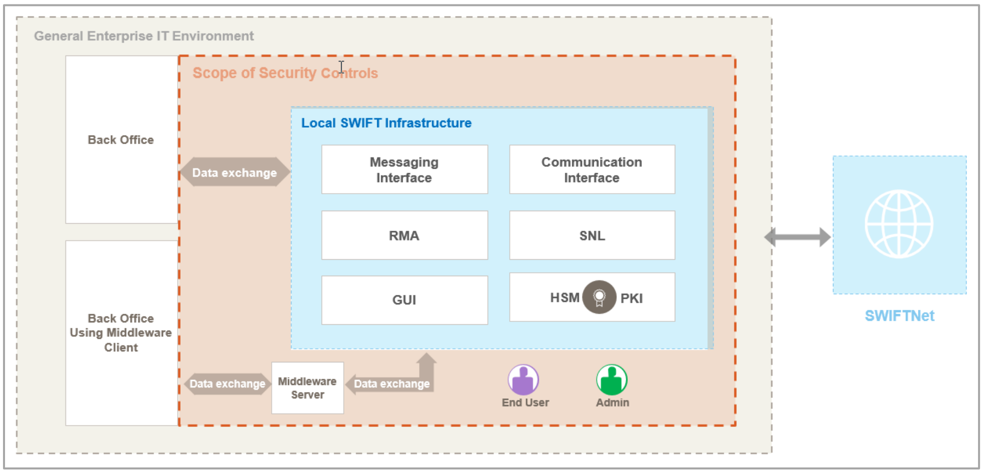

Figure 3a: Architecture A1 - Interfaces within the user environment

Users that do not operate or own a messaging interface but a communication interface only (such as in the figure below), are also considered as architecture A1.

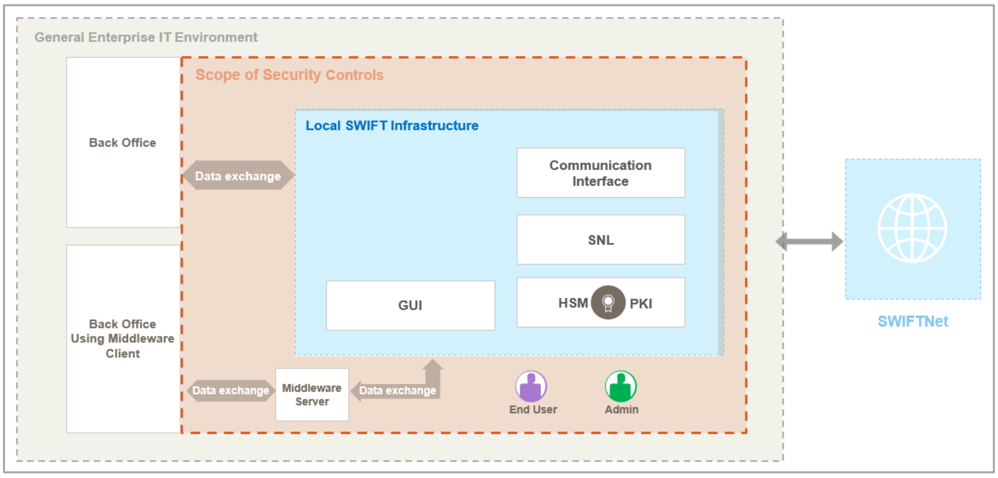

Figure 3b: Architecture A1 - Communication interface only within the user environment

This architecture type also includes hosted solutions where the user owns (has the license for) the communication interface that a) he operates on behalf of other user(s) or b) is operated for himself by a third party within or (hosted) outside the user environment.

- Architecture A2 – User owning the messaging interface without communication interface

  The messaging interface is owned, but a service provider (for example, a service bureau, SWIFT Alliance Remote Gateway or a group hub) owns the licence for and manages the communication interface.

  The below picture depicts the case where the communication interface is owned by and within the user environment.

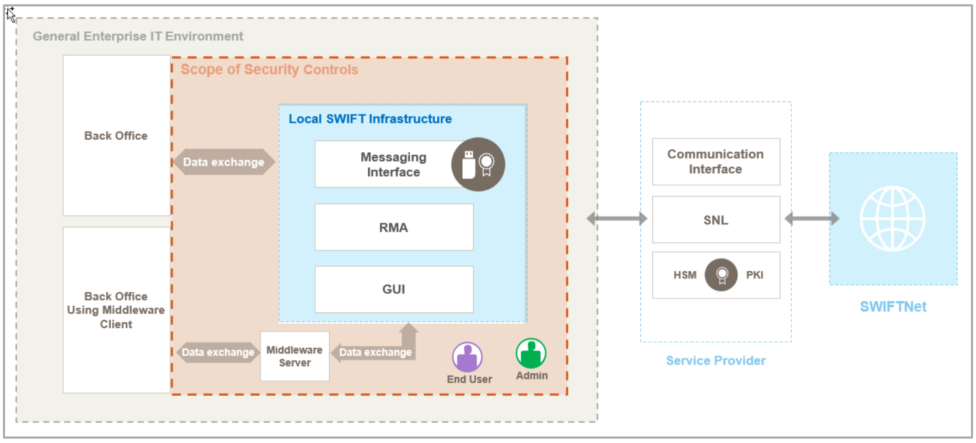

Figure 4: Architecture A2 – Messaging Interface only within the user environment

This architecture type also includes hosted solutions of the messaging interface where the user has the licence for the messaging interface.

- Architecture A3 – Connector (Figures 5)

  A software application (for example, Alliance Lite2 AutoClient, Direct Link or file transfer solutions – Figure 5a) or middleware systems (for example, IBM® MQ server or similar – Figure 5b) are used within the user environment to facilitate application-to-application communication with an interface at a service provider (for example, a service bureau, Alliance Lite2, a group hub). Optionally, this setup can be used in combination with a GUI solution (user-to-application).

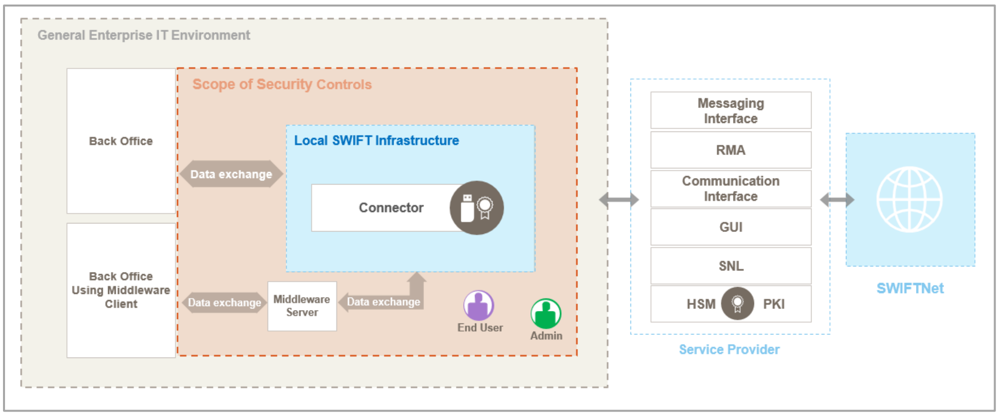

Figure 5a: Architecture A3 – Connector

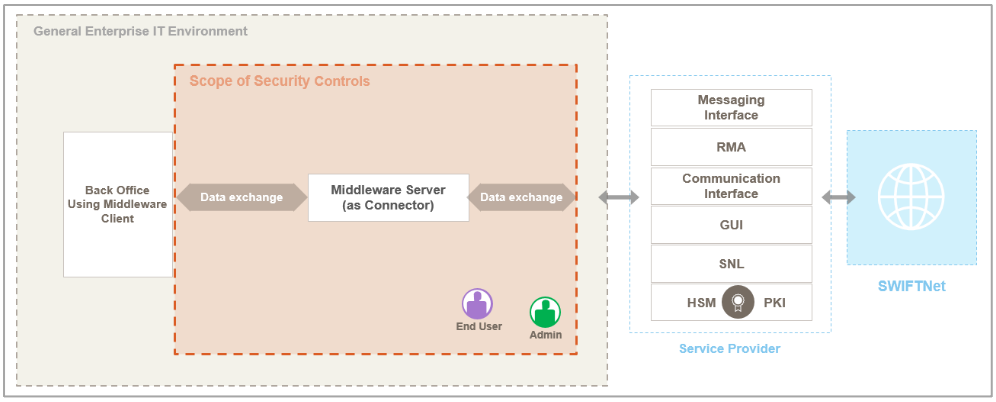
General Enterprise IT Environment
Scope of Security Controls
Back Office Using Middleware Client
Data exchange
Middleware Server (as Connector)
Data exchange
End User
Admin
Messaging Interface
RMA
Communication Interface
GUI
SNL
HSM
PKI
Service Provider
SWIFTNet

Figure 5b: Architecture A3 – Middleware as Connector

This specific architecture might require some attested B Architectures to be turned as A3. Those users would have to additionally consider and self-attest against the controls having middleware server in-scope.

- Architecture B – No local user footprint (Figure 6)

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

  - Users only access SWIFT services via a GUI application at the service provider (user-to-application). The PC or device used by those users should be considered as a (general purpose) Operator PC and protected accordingly.
  - Users' back office applications communicate directly with the service provider (application-to-application) using APIs from the service provider. Categorising this set-up as architecture type B is in line with the scope of the security controls, which excludes user back office applications. However, SWIFT strongly recommends implementing the architecture type A3 controls on these API applications.

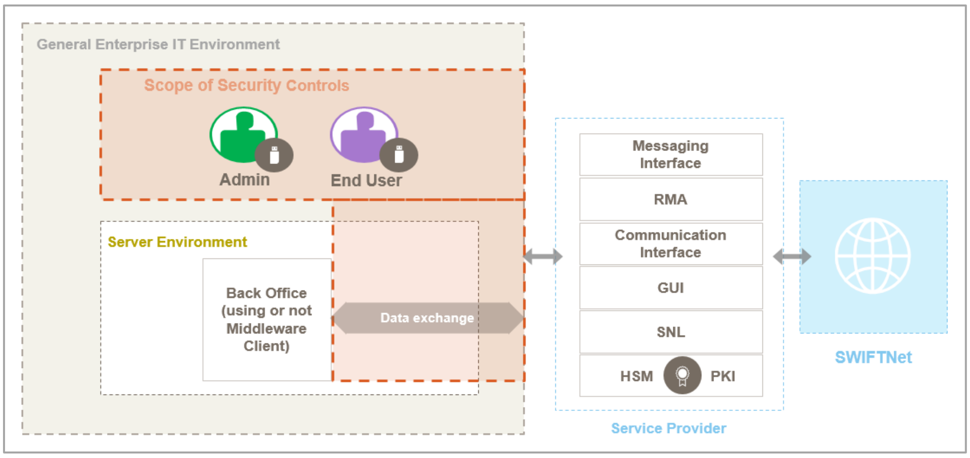

Figure 6: Architecture B - No user footprint

The security controls applicable for architectures A1, A2, and A3 are identical[1]. These architectures are referenced collectively on the following pages as type “A”. Fewer security controls apply to users that utilise architecture type "B”.

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

Security Controls Structure

Each security control in this document is structured into three parts: general control information, control definition, and implementation guidance, as described below.

General Control Information

- **Control Number and Title -** Each control has a unique number and title. If the control number is appended with an "A", this signifies that the control is "Advisory".
- **Control Type -** This identifies the control as "Mandatory" or "Advisory". Users must implement all Mandatory controls applicable to them taking into account their architecture type. Advisory controls are considered good security practice and are strongly recommended for additional implementation.
- **Applicability to Architecture types** - Controls are applicable either to users with architecture type A only or both types A and B. Users with type B architecture are not required to comply with controls applicable to type A only.

Control Definition

- **Control Objective** - States the security goal to be achieved irrespective of the implementation method.
- **In-Scope Components** - The specific SWIFT-related components that are covered by this particular control. (Also see Scope of Security Controls).

  Note: when extending scope to new components, these new in-scope components can initially be tagged as Advisory[2].
- **Risk Drivers** - Details the specific risks which are addressed by this security 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** - SWIFT-formulated method for control implementation.

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

[2] The Change Management process ensures 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:

1. Meets the stated control objective,
2. Addresses the risk drivers (see Appendix A for a risk matrix and Appendix C for illustrations of such risks), and
3. Covers the documented in-scope components relevant for the user's architecture.

The Control Statement is the suggested mean 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) Implementing a solution aligned with the implementation guidance provided in this document by SWIFT.

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

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

In such case, deployed controls, their effectiveness as well as particular environment specificities have to be taken into account to properly assess the control objective compliance of the solution (risk assessment approach).

Users are ultimately responsible for assessing the suitability of SWIFT-formulated implementation guidance in their environment or determining if they wish 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 routes 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 also shaded in the table below.

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

7.3A Penetration Testing	●	●
7.4A Scenario Risk Assessment	●	●

The following figures present visually where the controls would apply using for reference only one of many ways an architecture A1 could be designed (see also appendix B for some reference architectures).

Figure 7 presents the controls applied at the infrastructure and hosts level combined with organisational controls surrounding such environment. Figure 8 visualises the (interactive or application) flow controls between the SWIFT-related components and the Operator PCs or back office systems.

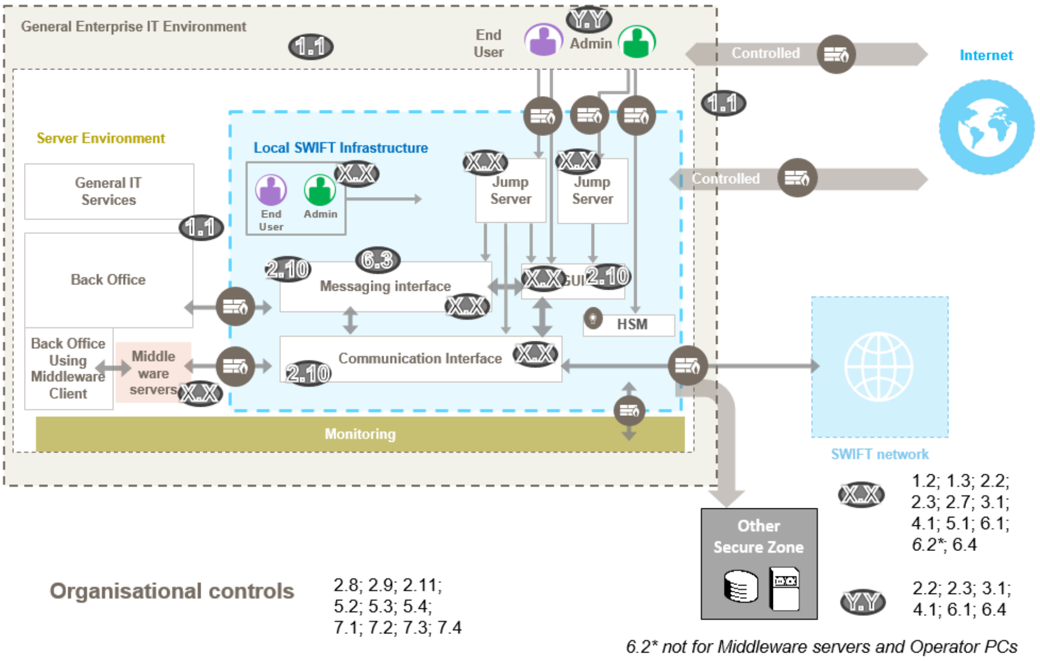

Figure 7: Infrastructure static and organisational controls

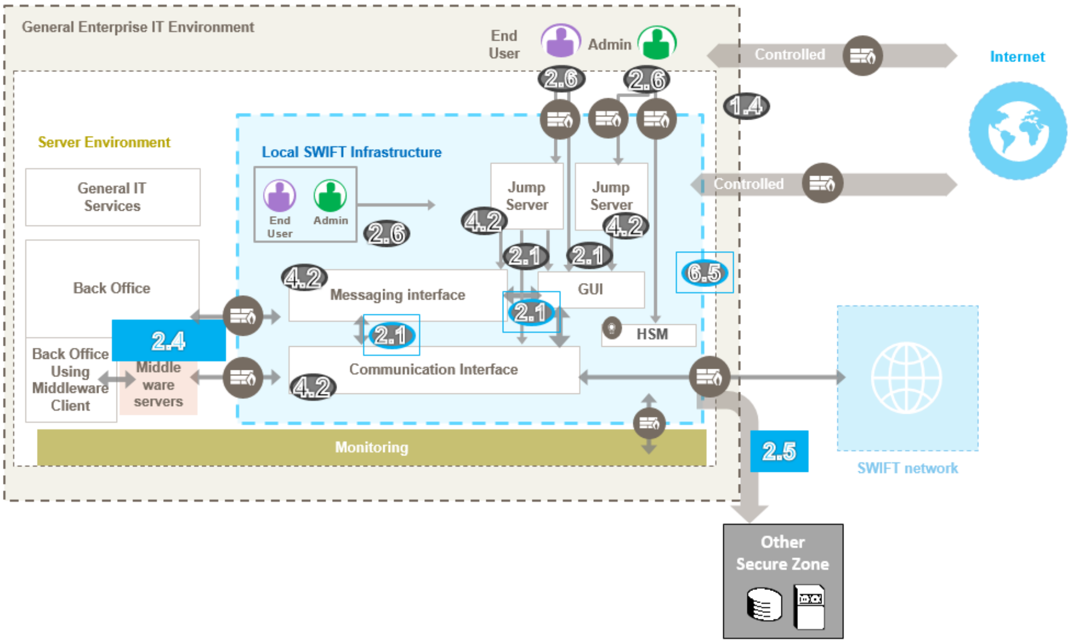

Figure 8: Human/Application to Machine/application flow controls

Detailed Control Descriptions

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

1.1 SWIFT Environment Protection

Control Type: Mandatory	**Applies to architecture:**	**A** ●	**B**

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)
- 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 segregated 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 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:

a) Overall design goals for implementing environment segregation

- 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 plaintext) in

Control Type: Mandatory	**Applies to architecture:**	**A** ●	**B**

systems outside of the secure zone. This does not apply to encrypted backup files. If the authentication services system is residing outside of the SWIFT secure zone:

  - 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 then the connectivity at the boundary of the secure zone). In such 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 scoped appropriate 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, trust and may communicate freely within the zone. Users may consider implementing additional segregation between components of the secure zone.
- Appendix B contains illustrative architecture diagrams showing samples of the many ways a secure zone may 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, communication interface, browser-based GUI, SWIFTNet Link, Hardware Security Module (HSM), connector, 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 server) 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 preferably fully segregated from production systems (incl. separate HSMs) and configured to only support test traffic (for example, by only using lite certificates and only configuring test logical terminals). If not fully segregated, 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 VPN boxes are in a secure environment with appropriate physical controls (in line with control 3.1).
- The secure zone size and scope is defined in a way that is most appropriate to the user's environment. Options may include, but are not limited to:
  - 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 email access).
- All messaging interface (Alliance Access and equivalent) and communication interface (Alliance Gateway and equivalent) products within the secure zone are SWIFT-certified. The list of certified interfaces is maintained and published by SWIFT on swift.com.

c) Protection of the secure zone

Boundary Protection

- Transport layer stateful firewalls are used to create logical separation 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. In case a firewall is shared to separate other zones, care must be taken for its management to ensure that compromise of the firewall should not affect the protection of the secure zone.

Control Type: Mandatory	Applies to architecture:	A ●	B

- ACLs, and application firewalls may be used to provide additional protections for the secure zone, but are not alone sufficient.

- Layer 2 devices (data link layer, such as switches) may be shared between the secure zone and other uses (VLAN segregation).
- 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 firewall(s) protecting the secure zone does not rely on the enterprise user authentication system but a system located on 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 all network flows are explicitly authorised (whitelisting). 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[3], inbound communications from approved general purpose operator PCs to the jump server, and outbound administration data (data logging, backups).
  - Firewall rules are reviewed at least annually.
  - 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 via 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:
    - Ensuring 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,
    - Restricting access to only authorised operators,
    - Removing any unnecessary software,
    - Restricting risky activity (for example: sending/receiving email),
    - No internet access,
    - Enabling logging.
  - Operators connect from their general purpose operator PC and only access the messaging or communication interface using a browser-based GUI (for example, Alliance Web Platform). Specific security controls apply to this setup:
    - Restricted internet access on the general purpose operator PC using one of the following options:
      1. No internet access
      2. Internet access using a remote desktop or virtual machine solution
      3. Internet access from the general purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
    - 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).
    - This set-up cannot be used for operating system administration activities.

[3] Multi-Vendor Secure IP Network

Control Type: Mandatory	Applies to architecture:	A ●	B

- 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 to the local network before accessing the secure zone via 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 use of virtual desktop infrastructure, dedicated channels for connectivity (for example, dedicated jump servers for remote users, leased lines).

e) Restriction of Internet access

- Internet access from systems within the secure zone (for example, the jump server or dedicated operator PCs) is highly restricted and ideally blocked.
  - Implementing a jump server architecture with no internet connection removes the requirement to restrict internet access on connected individual general purpose operator PCs.
- 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 patches for secure transfer into the secure zone.
- If internet access is needed from within the secure zone, access should be granted only to whitelisted URL destinations via a proxy with content inspection and adequate blocking/filtering controls. Connections are only permitted if initiated in the outbound direction.
- General purpose internet browsing from within the secure zone is not permitted.

f) Segregation from General Enterprise IT Services

- To protect the secure zone from credential theft and/or compromise of enterprise authentication (LDAP, RADIUS, multi-factor) services, 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 ensuring that these systems do not store authenticators (passwords, tokens, etc.) for systems and accounts in scope in any format (hashed, encrypted, plaintext) outside of the secure zone or another existing secure zone that has similar controls. Indeed, the supporting IT infrastructure need 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 whitelisting, allowing only trusted applications to be executed.
- Restrict the communication between components in the secure zone considering:
  - Network ACLs or host-based firewalls restricting 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 their organisation may consider implementing alternative controls such as those suggested below. The specific alternative solutions must be risk-appropriate to each environment, and consider the effort required to effectively implement, manage, and maintain the solution.

- Not segregating 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 crossing the secure zone boundary. Controls may include: locating the authentication service within an existing secure zone that has similar controls as the ones 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,

Control Type: Mandatory	Applies to architecture:	A ●	B
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, boundary firewall management) are shared between the secure zone and other environments, any credentials used across the environment should be monitored to ensure they are only used when and where expected. • If a general enterprise server is initially used to reach the secure zone, that server is only used to filter legitimate connectivity access. Identity and access management for secure zone components and/or the jump server still relies on authentication services residing 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, the user must ensure that any compromise of such functions will not compromise the security of the in-scope components.			

1.2 Operating System Privileged Account Control

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	

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

In-scope components:

- Secure zone: administrator-level operating system accounts (on physical or virtual machines)
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM’s: platform administrator-level accounts
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

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 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, deleting evidence).

Implementation Guidelines:

- Administrator-level accounts are defined as:
  - 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.
- Access to administrator-level operating system accounts is restricted to the maximum extent possible unless needed to install, configure, maintain, operate and support emergency activities. The use of the administrator-level account is limited to the duration of the activity (for example, maintenance windows).
- Log-in with built-in administrator-level accounts is 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.

<table>
<tr><td><b>Control Type: Mandatory</b></td><td><b>Applies to architecture:</b></td><td><b>A</b>
●</td><td><b>B</b></td></tr>
<tr><td colspan="4"><b>Optional Enhancements:</b>
• Systems are configured to not allow log-in of built-in administrator-level accounts, except via a maintenance mode (for example, single user mode or safe mode). This effectively prohibits logging into the account as a service, batch job, through remote desktop services, or by escalating privilege from another account.</td></tr>
</table>

1.3 Virtualisation Platform Protection

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	

Control Objective: Secure virtualisation platform and virtual machines (VM's) hosting SWIFT related components to the same level as physical systems.

In-scope components:

- Virtualisation platform (also referred as the hypervisor) and VM's used to host any of the below SWIFT related components:
  - Messaging interface
  - Communication interface
  - GUI
  - SWIFTNet Link
  - Connector
  - Jump server
  - Dedicated and general purpose operator PCs
  - Firewalls
  - [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

Risk Drivers:

- Unauthorised access
- Uncontrolled proliferation of systems and data

Implementation Guidance

Control Statement:

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

Control Context:

Security controls that apply to non-virtualized (i.e. physical) systems are equally applicable to virtual systems. The additional virtualisation layer needs extra attention from a security point of view. Uncontrolled proliferation of VM's could lead to unaccounted-for machines with the risk of unmanaged, unpatched systems open to unauthorised access to data,

Providing appropriate controls have been implemented to this underlying layer, 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 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, location in an existing secure zone that has similar controls as the ones applicable to the SWIFT secure zone, privileged access restrictions, log-in and password policy, installation of security patches, and restriction of internet access. Those controls have the virtualisation platform identified in their "In-scope components" section.
- Vulnerability scanning is performed on SWIFT-related VM's and when technically possible on the virtualisation platform.
- The virtualisation platform hosts are subject to physical protection preventing unauthorised physical access.
- VM's isolation is ensured on the virtualisation platform to prevent a) lateral move out of a virtual machine to access or interact with other VM's or the underlying hypervisor or b) bypassing normal network controls that

Control Type: Mandatory	Applies to architecture:	A ●	B

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

- If multi-factor authentication is implemented for interactive access to the SWIFT related VM's operating systems, in line with control 4.2, preventing direct access to those VM's from the hypervisor layer, multi-factor authentication is not mandated at the virtualization platform management level.

1.4A Restriction of Internet Access

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

Control Objective: Restrict Internet access from operator PCs and other systems within the secure zone

In-scope components:

- Dedicated and general purpose operator PCs
- Jump Server
- Middleware server (such as IBM® MQ server or similar) used to exchange with SWIFT-related components
- Virtualisation platform (also referred as the hypervisor)
- Messaging interface
- Communication interface
- GUI
- SWIFTNet Link
- Connector

Risk Drivers:

- Exposure to internet-based attacks

Implementation Guidance

Control Statement:

All operator PCs and systems within the secure zone have restricted direct internet access in line with business.

Control Context:

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

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

This control centralises elements from the mandated control 1.1, and some additional considerations. Once this control is turned to Mandatory, the redundant information will be removed from 1.1.

Implementation Guidelines:

a) Internet access from the secure zone

- General purpose internet browsing (including Web Mail activities) from systems within the SWIFT 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 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 patches for secure transfer into the secure zone.
  - If internet access is needed from within the secure zone, access should be granted only to whitelisted URL destinations via a proxy with content inspection and adequate blocking/filtering controls. Connections are only permitted if 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 Operator PCs

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

- Restrict internet access on the general purpose operator PCs used to connect a GUI application at the service provider (user-to-application) as part of an Architecture B. Use one of the following options:

  1. Internet access through a remote desktop or virtual machine solution
  2. Internet access from the general purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
- Restrict internet access on the general purpose operator PC used to access a messaging or communication interface through a browser-based GUI (for example, Alliance Web Platform). Use one of the following options:
  1. Internet access through a remote desktop or virtual machine solution
  2. Internet access from the general purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
  3. No Internet access
- Enforced usage of a jump server with no internet access combined with multi-factor authentication implemented on the individual SWIFT related applications/systems or at the jump server as per control 4.2 remove the need to restrict internet access on the general purpose operator PC. SWIFT still strongly suggest considering restricted internet access for those PCs.

c) Internet Access from other components

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

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

2 Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security

Control Type: Mandatory	Applies to architecture:	A ●	B

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

In-scope components:

- Jump server when used
- SWIFT-related infrastructure 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-to-application and, when used, jump server-to-application, data flows.

Control Context:

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

Implementation Guidelines:

- All data flows between SWIFT-related applications are protected using a secure mechanism (for example, "Local Authentication (LAU) in combination with a confidentiality protection" or "2-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.
- 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, integrity and authentication of the connection to the application.
- Secure protocols use current, commonly accepted cryptographic algorithms (for example, AES[4], ECDHE[5]), with key lengths in accordance with current best practices. More guidelines on cryptographic algorithms supporting secure protocols can be found in SWIFT Knowledge Base TIP 5021566.

[4] Advanced Encryption Standard

[5] Elliptic Curve Diffie-Hellman Ephemeral

2.2 Security Updates

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

Control Objective: Minimise the occurrence of known technical vulnerabilities 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:

- Operator PC and, when used, jump server: all hardware and software
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM's
- Secure zone: all hardware including network devices and software
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

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 lifecycle 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 patches are available.

Implementation Guidelines:

- Vendor support
  - All software (including operating systems) and hardware (including network devices) are within the actively supported product lifecycle 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/patches. Risk assessment considerations may include: the vendor-reported criticality of the patch, user exposure and vulnerability, mitigating controls, and operational impact.
  - User-defined deployment timelines are established for applying patches based on criticality, system type, and required patch testing.
  - In the absence of established internal processes and timelines, SWIFT recommends the use of Common Vulnerability Scoring System (CVSS) Version 3 as a guideline for criticality, with the following patch deployment targets:
    - Critical (9.0+ score): applied within 1 month of release
    - High (7.0 - 8.9 score): applied within 2 months of release
    - Low / Medium (< 7.0 score): user defined.

<table>
<tr><td><b>Control Type: Mandatory</b></td><td><b>Applies to architecture:</b></td><td><b>A</b>
●</td><td><b>B</b>
●</td></tr>
<tr><td colspan="4">– Note: It is common practice that operating system security updates/patches are usually 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, their legitimate source is validated and integrity checks (for example checksum validation) performed when technically possible.</td></tr>
</table>

2.3 System Hardening

Control Type: Mandatory	Applies to architecture:	A ●	B ●

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

In-scope components:

- Operating systems for Operator PC and when used jump server
- Operating systems for SWIFT-related applications (including VM’s)
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM’s
- Supporting infrastructure within the secure zone (for example, firewalls, routers)
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

Note: SWIFT HSMs are FIPS 140-2 Level 3 compliant with hardened underlying OS and are out of 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:

- All in-scope systems are hardened considering one or more of the following:
  - Vendor security configuration guidance,
  - Industry-standard security configuration guidance (for example,[6] CIS , DISA STIG, NIST),
  - A local or regulator's standard security configuration or controls set of the same rigour as the vendor or industry guidance.
- 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:
  - 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, USB) as appropriate,

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

Control Type: Mandatory	Applies to architecture:	A ●	B ●
– Set, when technically possible, auto-lock options (such as activating an Operator PC screen saver requiring to sign-in again after an inactivity time-out or once turned into 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 on accomplishing 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: – By checking regularly, at least twice a year, the systems against the secure settings identified as per preceding guidance to take any relevant corrective actions – Or by regularly applying the identified secure settings to the systems.			

2.4A Back Office Data Flow Security

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

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

In-scope components:

- Data exchange layer: flows of financial transactions between the SWIFT-related components and the back office first hop 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 mutual or message level based authentication mechanisms are implemented to protect data flows between SWIFT infrastructure components and the back office first hop they connect to.

Control Context:

Protection of data flows/connections between the back office first hop, as seen from the SWIFT secure zone, and the SWIFT infrastructure safeguards against man-in-the-middle, unintended disclosure, modification, and data access while in transit.

Implementation Guidelines:

- Data flowing between SWIFT-related components 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, 2-way TLS) that provides confidentiality, integrity, and mutual authentication of the data in transit. This includes the data flow between:
  - 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[7], ECDHE[8]), with key lengths in accordance with current best practices. More guidelines on cryptographic algorithms supporting secure protocols can be found in SWIFT Knowledge Base TIP 5021566.
- As this control is expected to be (gradually) turned Mandatory in a future release, following guidelines are already provided to gradually reach compliance:
  - Have an inventory of data flows between SWIFT related components and the first back office (or middleware) hops
  - Have a plan to implement/activate secure mechanisms for identified flows considering
    - Implementing secure mechanisms (see first bullet above) as exposed by the interfaces, connectors or middleware server
    - Migrating opportunistically legacy and less standard flows to secure mechanisms or protocols
    - Mitigating, in the meantime, the risk of back office host spoofing or messages injection through

[7] Advanced Encryption Standard

[8] Elliptic Curve Diffie-Hellman Ephemeral

Control Type: Advisory	Applies to architecture:	A ●	B ●

systems or network connectivity means.

- When a middleware is used, some requirements are expected on the middleware server hosts; they are indeed the guardians of the connections between the back office and the SWIFT-related components:
  - Irrespective of where the middleware server hosts are located and shared with, the same security requirements apply to those hosts as for other SWIFT-related components or infrastructure systems. Those security requirements cover: location in another secure zone that has similar controls as the ones applying to the SWIFT secure zone, privileged access restrictions, log-in and password policy, installation of security patches, restriction of internet access. Those controls have, Advisory so far, middleware server identified in the “In-scope components” of their control definition.
  - Protection of the data on the middleware servers (such as when in the MQ queues) has to be ensured to prevent unauthorised access (for instance by implementing thorough access control and opportunistically queues or data at rest encryption)
  - Protection of the SWIFT related data flowing between the middleware server hosts (such as between several in series MQ servers) should be ensured as part of the middleware infrastructure protection by using secure mechanisms (see first bullet of the implementation guidelines above)
  - Definition and management of the connectivity rules and business flows on the middleware servers have to be secured to prevent unauthorised flows
- For middleware applications (such as IBM® MQ) directly connecting to SWIFT infrastructure components, it is advised to also implement the same level of protection between this middleware layer and the back office first hop as seen from an application point of view by the SWIFT-related component. In order to gradually reach compliance for those links following guidelines are already provided:
  - Have an inventory of SWIFT-related data flows between middleware server and the back office first hops as seen from SWFIT-related component
  - Have a plan to implement/activate secure mechanisms for identified flows considering
    - Implementing secure mechanisms (see first bullet of the implementation guidelines above) as exposed by the middleware server or the back office system
    - Opportunistically migrating legacy and less standard flows to secure mechanisms or protocols
    - Ensuring, in the meantime, authentication of the data sources and authorisation of the SWIFT-related data through a) native middleware functionalities or b) systems or network connectivity means preventing host spoofing.

Note: SWIFT expects this control to become mandatory in a future version of this document by phasing the expectations: starting with, when used, middleware server and flows towards the SWIFT-related components and closing with the SWIFT-related flows towards the back office systems reached by the SWIFT-related components directly or via the middleware server.

2.5A External Transmission Data Protection

Control Type: Advisory	Applies to architecture:	A ●	B

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 backup data
- Loss of sensitive data confidentiality

Implementation Guidance

Control Statement:

Sensitive SWIFT-related data leaving the secure zone as the result of (i) operating system/application backups, business transaction data replication for archiving or recovery purposes or (ii) extraction for off-line processing is protected when stored outside of a secure zone and 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 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 backups and replication of business transaction data can provide useful information to prepare fraudulent transactions. Their transfer and storage outside of secure zones (when, for example, using the SAN/NAS[9] technology), have therefore to 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 control are usual means to protect stored data.

Off-line processing covers for example processing performed for support activities, additional analysis or business intelligence activities.

Implementation Guidelines:

- Replicated or extracted SWIFT-related sensitive data (business transaction data revealing details such as involved debtors, creditors, accounts, amounts, trade information), passwords and other authenticators is :
  - Protected from unauthorised access when stored outside of the SWIFT secure zone or another secure zone that has similar controls as the SWIFT secure zone. Such replicated or extracted data set is also ideally encrypted when stored outside of a secure zone (this can be achieved either at data, file, application or system level),
  - 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.
- Encryption protocols or mechanisms use a current, commonly accepted cryptographic algorithm (for example, AES[10], ECDHE[11]), with key lengths in accordance with current best practices. More guidelines

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

[10] Advanced Encryption Standard

[11] Elliptic Curve Diffie-Hellman Ephemeral

on cryptographic algorithms supporting currently secure protocols can be found in SWIFT Knowledge Base TIP 5021566.

- Encryption mechanisms comply with applicable laws and regulations.
- If the cryptography protecting SWIFT-related sensitive data has been compromised, a process should be established to apply new cryptography and secure or destroy any compromised copies of the data.

Note: It is expected that backups kept for business or system recovery are maintained in a secure zone that has similar controls as the SWIFT secure zone.

2.6 Operator Session Confidentiality and Integrity

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

Control Objective: Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.

In-scope components:

- Operator PC and when used jump server: sessions to operating system or to the virtualisation platform management console (also called hypervisor manager)
- Operator PC and when used jump server: sessions to interface applications in the secure zone or at the service provider
- Secure zone: session to HSM and SWIFT-related applications and operating systems from dedicated operator PCs
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with 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 connecting to SWIFT-related applications or into the secure zone is safeguarded.

Control Context:

Operator sessions, via the jump server when used, with the local or external SWIFT infrastructure pose a unique threat because unusual or unexpected activity is harder 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 passwords theft. When used, access to the virtualisation layer (hypervisor manager) has to be similarly protected.

Implementation Guidelines:

- 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[12], ECDHE[13]), with key lengths in accordance with current best practices. More guidelines on cryptographic algorithms supporting secure protocols can be found in SWIFT Knowledge Base TIP 5021566.
- Operator sessions and other session types (for example, admin or maintenance) have an inactivity lock-out feature that limits the session to the minimal timeframe necessary to perform business-as-usual duties.
- If the inactivity lock-out is not implemented at the application level, it should be implemented at the operating system-level of the application, or on the jump server.

[12] Advanced Encryption Standard

[13] Elliptic Curve Diffie-Hellman Ephemeral

2.7 Vulnerability Scanning

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

- Operator PC (or jump server)
- Secure zone: all SWIFT-related applications and operating systems including also dedicated operator PCs
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

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:

- Vulnerability scanning is performed at least annually as well as after any significant change to the environment (for example, new server components, network design change).
  - Vulnerability scanning tools are from a reputable vendor and updated with scan profiles within one month prior to scanning.
  - The most appropriate type of vulnerability scanning (such as using credentials or black-box) 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 ideally real-time scanning is recommended.

Optional Enhancements:

- Vulnerability scanning should include network components (such as routers and switches).
- Vulnerability scanning includes general operator PCs or, as an alternative, security patches are regularly applied on the general operator PCs. In the latter case, only supported and regularly patched applications are deployed on those PCs.

2.8A Critical Activity Outsourcing

Control Type: Advisory	**Applies to architecture:**	**A** ●	**B** ●

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

In-scope components:

- Organisational control

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, such as network and system maintenance, are outsourced to a third party (for example, external IT provider, cloud computing provider, service bureau, or 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 ensure that no new weaknesses or vulnerabilities are introduced.

Note:

- SWIFT defines the following operations as critical:
  - Security management and change management of the hardware and software (including applications and operating system) supporting the SWIFT service,
  - RMA-related operations,
  - Accessing sensitive user data (for example, message content),
  - Monitoring of events containing 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:

- When outsourcing its SWIFT–related infrastructure or part of it to a third party (such as an external IT provider or cloud computing provider) acting on his behalf, the user remains responsible for the conformance with the security controls of this framework and must seek compliance from their third party.
- When the third party provides shared services to connect not-related SWIFT users, the third party must be registered to the Shared Infrastructure Programme or the Alliance Lite2 for Business Applications programme. The user is still responsible for his own infrastructure and organisation.
  - Service bureaux registered and compliant under the Shared Infrastructure Programme are listed in the SWIFT Partner Programme Service Bureau Directory
  - Lite2 for Business Applications providers registered and compliant under the related programme are listed in the Lite2 Business Applications Providers Directory
- Service Level Agreements (SLA) and a Non-Disclosure Agreement (NDA) are established with any third party to whom critical activities have been outsourced. These SLA define the standard of care under which those critical operations are carried out by the third party.

Control Type: Advisory	Applies to architecture:	A ●	B ●
- A risk assessment of the third party is conducted at the start of the engagement, and reviewed on a regular basis thereafter.			

2.9A Transaction Business Controls

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

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

In-scope components:

- GUI
- Secure zone: messaging interface
- Secure zone: communication interface
- Secure zone: connector

Note: Components are mentioned as the vector for transaction business controls

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 transaction activity to within the expected bounds or normal business.

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 normal business activity. Parameters can then be set to restrict business to acceptable thresholds based on 'normal' activity.

Implementation Guidelines:

- Implement controls that will detect, prevent, or additionally validate the flow of transactions against expected bounds of normal business (payment controls service). Examples include:
  - SWIFT transaction submission and approval is restricted outside of normal business. In cases of 24-hour centralised SWIFT processing, restrict or monitor transactions as appropriate to support business as usual: suspicious messages can also be blended in with legitimate traffic.
  - Have a process in place to issue and check confirmation messages (for example, to check that the MT900 and MT910 confirmations match the transactions which have occurred on the accounts),
  - Reconciliation of the entity's accounting records with end-of-day statement messages (for example, MT 940 and MT 950),
  - Reconciliation is performed daily between the messages that are sent to/from the back office and to/from the SWIFT Network,
  - Session numbers within the messaging interface are tracked to ensure that the sequential session numbering is intact with no unexpected gaps,
  - Limit active SWIFTNet FIN sessions to business hours (for example, automated logical terminal sessions log out at end of business day). In cases of 24-hour centralised SWIFT processing, restrict or monitor transactions as appropriate to support business as usual,
  - Monitor uncharacteristic transactions (for example, exceptionally high amounts or cumulative amounts, unusual beneficiaries, senders or currencies).
- Alternatively or in addition, independent reconciliation is undertaken with users' transaction data securely obtained from a secondary source (either internal or external such as SWIFT daily validation reports) or by verifying, the transaction is genuine with the emitter and/or the recipient.

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

Optional Enhancements:

- Application and operating system accounts are restricted from log-in attempts that occur outside of expected role-specific operational hours.

2.10 Application Hardening

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	

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

In-scope components:

- Messaging interface
- Communication interface
- GUI
- SWIFTNet Link
- Connector

Risk Drivers:

- Excess attack surface
- Exploitation of insecure application configuration

Implementation Guidance

Control Statement:

All messaging interfaces and communication interfaces products within the secure zone are SWIFT-certified. 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 a malicious person may use during an attack. It also ensures that potential default credentials are changed.

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

Implementation Guidelines:

- Ensure the messaging and communication interfaces are SWIFT-certified (the list of certified interfaces is published in the Certification Register on www.swift.com).
    - The SWIFT-certified interface should meet all the security conformance requirements (mandatory and advisory) defined in the SWIFT Certified Interface Programme.
        - If some security conformance requirements are yet to be met, the user should upgrade to a certified interface implementing at least the minimum mandatory security conformance requirements.
        - The interface provider should be contacted in case of doubt 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 SWIFT Alliance Security Guidance),
    - A local or regulator's standard security configuration or controls set of the same rigour as the vendor guidance.
- At a minimum, the application hardening process should:
    - Change default existing passwords,
    - Disable or remove unnecessary user accounts,

Control Type: Mandatory	Applies to architecture:	A ●	B

- – Disable or restrict unnecessary components, adaptors or connectors,
- – Configure securely the adapters, connectors or remote connections,
- – Remove unnecessary packages,
- – Adjust any default configurations known to be vulnerable.

- Deviations from the selected hardening configuration (i.e. a set of rules) are documented along with the justification for the deviation.

Optional Enhancements:

Additional applications installed on the in-scope components and handling 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:**	**A** ●	**B** ●

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

In-scope components:

- GUI
- Secure zone: messaging interface

Note: GUI and messaging interface are mentioned as the vector for 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.

Implementation Guidelines:

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

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

3 Physically Secure the Environment

3.1 Physical Security

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

- Operator PC and when used jump server), including removable equipment
- Secure zone: all hardware
- Hardware supporting virtualisation platform (also referred as the hypervisor) and hosting SWIFT-related VM's
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

Note: Alliance Connect VPN boxes are generally out of scope but expected to be in an environment with appropriate physical controls as described here 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:

- Security of Removable Equipment
  - Sensitive removable equipment (for example, PIN Entry Device (PED), PED keys, SWIFT-related smart cards, USB Tokens, TOTP Devices) is supervised or securely stored when not in use.
  - Sensitive removable equipment required for normal continuous operations (for example, hot swappable disks, 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 accessing SWIFT systems is not required.
  - Printers used for SWIFT transactions are located in a secured workplace environment and their access is restricted.
  - USB and other external access points on operator PCs are disabled to the maximum extent possible, while still supporting operations (for example, when tokens are required to authenticate users or message operations).

Control Type: Mandatory	Applies to architecture:	A ●	B ●

- Security for Remote Workers (for example, teleworkers, "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 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. 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 at least annually.

4 Prevent Compromise of Credentials

4.1 Password Policy

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

- Log-in to Operator PC and when used jump server
- Secure zone: application and operating system accounts
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM's
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]
- 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 log-in attempts. Similarly, personal tokens and mobile devices enforce passwords or 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.

It is however 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 multifactor authentication requirement.

Implementation Guidelines:

- A password policy covering also 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 reuse,
  - Lockout after failed authentication attempts, and remedy.
  - Password requirements may be modified as necessary for specific use cases:
    - In combination with a second factor (for example, one-time password),
    - Authentication target (for example, operating system, application, mobile device, token),
    - Type of account (general operator, privileged operator, application-to-application account or local authentication keys).

  More good practice guidelines on password and PIN parameter settings can be found in SWIFT

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

Knowledge Base TIP 5021567 and 5022038.

- The password policy is developed in consideration of known password-based vulnerabilities in the computing environment. For example, requiring a 15+ character password for Windows systems prevents Windows from computing the highly vulnerable LM (LAN Manager) password hash.
- The established password policy is enforced through technical means (for example, through Active Directory group policy, or within application settings) where possible.
- Effectiveness of the password policy is reviewed regularly (recommended annually).
- 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: It is important that users implement strong passwords, and preferably strong authentication, for all systems used within the end-to-end transaction chain, and not limit these controls to only the SWIFT infrastructure.

4.2 Multi-factor Authentication

		A	**B**
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

Depending on implementation:

- Dedicated operator PC log-in
- Operator access to jump server
- Operator log-in process to the messaging interface (incl. hosted DB) and communication interface
- Operating system hosting the messaging interface (incl. hosted DB) and communication interface

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 applications and operating system accounts.

Control Context:

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

- Knowledge factor (something the operator knows), typically, a password.
- Possession factor (something the operator has), typically:
  - connected tokens (for example, USB tokens, smartcards),
  - disconnected tokens (for example, one-time password generators using operators’ mobile phone, RSA token or Digipass).
- Inherence factor (something the operator is), typically, biometrics such as fingerprint, 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 compromise. Attackers often use the privileges of a compromised account to move laterally within an environment and progress an attack.

Implementation Guidelines:

- 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 deemed sufficient to access the local SWIFT systems.
    - Second factor solutions based on a possession factor include (not exhaustive list): TOTP, RSA SecurID, Digipass, Mobile App, Transaction Authentication Number (TAN) Table, personal USB token. Solution to be selected as per user's own risk management.

  - An inherence factor is more safely combined with a possession factor than with a knowledge factor.
- Multi-factor authentication is implemented at least on one authentication stage/step faced by the end user when accessing a SWIFT application:
  - For operating system administrators:
    - At the secure zone boundary (jump server),
    - At the dedicated operator PC log-in (within the secure zone).
  - For end users in descending order of security robustness:
    - On the individual SWIFT applications (on the browser-based GUI, on the messaging interface, or on the communication interface),
    - At the secure zone boundary (jump server),
    - At the dedicated operator PC log-in (i.e. 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 feasible, the authentication system supporting the multi-factor solution is located within the secure zone.
- The authentication factors presented are individually assigned and support individual accountability of access to services, operating system, and applications.
- If single sign-on (for example, SAML) is implemented, then a second factor is still required at the single sign-on, or at a later stage.

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

5 Manage Identities and Segregate Privileges

5.1 Logical Access Control

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

- All operator accounts (for example, virtualisation platform, also referred as the hypervisor, hosting SWIFT-related VM’s, VM’s themselves, operating systems, applications and HSM)
- [Advisory : All operator accounts on the middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

Risk Drivers:

- Excess privilege or access
- Segregation of duty violations
- Unauthorised access

Implementation Guidance

Control Statement:

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

Control Context:

Applying the security principles of (1) need-to-know, (2) least privilege, and (3) segregation 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 accounts as part of an attack.

Implementation Guidelines:

A logical access control policy is documented and enforced to consider 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 ensures 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 ensures that user and administrator privileges are controlled in a way that allows all privileges to be tailored to individual needs.
  - Accounts are granted only the privileges that are required for normal, routine operation. Additional privileges are only granted on a temporary basis.
- Segregation of Duties and 4-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.

Control Type: Mandatory	**Applies to architecture:**	**A** ●	**B** ●

- – Sensitive permissions are separated to prevent by-passing the 4-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 are promptly revoked when an employee changes roles or leaves the organisation.
  - – Accounts are reviewed at least annually (ideally more frequently) and adjusted as required to enforce access security principles.
- An emergency procedure to access privileged accounts is documented for use when authorised persons are unavailable due to unexpected circumstances:
  - – Any operational use of the procedure is logged.
  - – Access to the emergency privileged accounts is controlled. The usage is logged and the password is changed after emergency use.

5.2 Token Management

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

- Connected hardware authentication 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 hardware authentication tokens are managed appropriately during assignment, distribution, revocation, use, and storage.

Control Context:

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

Implementation Guidelines:

- A controlled process is used for the assignment and distribution of connected hardware tokens used for SWIFT operations (for example USB token, HSM token, smart card).
- Token assignment is reviewed at least annually (ideally more frequently).
- Personally assigned hardware tokens are revoked when the individual no longer requires access and should possibly be recalled (for disposal or reassignment as appropriate).
- A record is maintained of assigned hardware tokens 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 and access is tracked)
  - 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 asking to limit software deployed on the remote PC. Such PC should be dedicated to remote PED activities and not a standard General Purpose Operator PC.

5.3A Personnel Vetting Process

		A	B
Control Type: Advisory	**Applies to architecture:**	●	●

Control Objective: Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting in line with applicable local laws and regulations.

In-scope components:

- All personnel (such as employees, agents, consultants and contractors) with operational (maintenance or administration) access to SWIFT-related systems and virtualisation platform hosting SWIFT-related VM's

Risk Drivers:

- Untrustworthy staff or system operators

Implementation Guidance

Control Statement:

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

Control Context:

A personnel vetting process, 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:

To the extent permitted under applicable laws and regulations and to the extent the information is available, the below guidelines and specified verifications are recommended:

- All in-scope personnel are vetted at least every 5 years.
  - For those already in the role and not yet vetted, a catch-up process is gradually organised as part of the periodic vetting (sometimes also referred to as re-vetting)
- The vetting process for initial employment includes the following verifications (to be conducted in accordance with applicable local laws and regulations[14]):
  - 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,
  - Financial credit verification.
- The periodic vetting process includes the following verifications (to be conducted in accordance with applicable local laws and regulations[15]):
  - 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.

[14] Including, where applicable, social concertation

5.4 Physical and Logical Password Storage

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	●

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

In-scope components:

Accounts and passwords defined on the following components:

- Operator PC and when used jump server: for operating system access
- Operator PC and when used jump server: interactive user session
- Secure zone: all applications, operating systems, HSM and related tokens and network components
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM's
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]
- SWIFTNet Online Operations Manager 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) ensures that passwords are not easily accessible to others, thereby protecting against simple password theft. Common unsecure methods include (unexhaustive list): recording passwords in a spreadsheet or a text document saved in clear on a desktop or in a shared directory or a server, saved in 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 can be damageable, such as transaction creator account and approver account (ii) even monitoring accounts provide valuable information during the reconnaissance time.

Implementation Guidelines:

- Passwords written on physical media are protected via:
  - Placement inside a sealed, tamper-evident security envelope,
  - Storage in a certified safe (for example, Underwriters Laboratories (UL) Class TL or EN-1143-1 certification),
  - Logging of access to the storage location and which account's password was accessed.
- Passwords stored logically (digitally) are protected via:
  - Encryption-at-rest or obfuscation (that is, no plain-text storage),
  - Authenticated access to the storage location, ideally with logging of access.
- Passwords are not recorded in user manuals or other operational material unless the password is stored in accordance with the guidance above.
- If emergency access is granted to an operator who under normal conditions would not have access, 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.

6 Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection

Control Type: Mandatory	Applies to architecture:	A ●	B ●

Control Objective: Ensure that local SWIFT infrastructure is protected against malware.

In-scope components:

- Operator PC and when used jump server - Windows operating systems
- Secure zone: SWIFT-related servers - Windows operating systems
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components – Windows operating systems]
-

Risk Drivers:

- Execution of malicious code
- Exploitation of known security vulnerabilities

Implementation Guidance

Control Statement:

Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.

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:

- 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 and/or outside of business hours.
- 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 setup, 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 raising an alarm to 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 in case it is confirmed they are legitimate.
- Ensure that the transfer of any file content does not contain any kind of virus or other data that may create risks for the sender, for SWIFT, or for the receiver.

Optional Enhancements:

- Anti-malware systems use a combination of signature-based and heuristic-based capabilities.
- Anti-malware solutions are implemented on non-Windows systems.
- On-demand full scanning is scheduled at least on a weekly basis on servers.

6.2 Software Integrity

		A	B
Control Type: Mandatory	**Applies to architecture:**	●	

Control Objective: Ensure the software integrity of the SWIFT-related applications.

In-scope components:

- Secure zone: connector
- Secure zone: GUI to the messaging and communication interface
- Secure zone: messaging interface application
- Secure zone: communication interface application
- Secure zone: RMA
- Secure zone: SNL

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.

Control Context:

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

Implementation Guidelines:

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

  Options for implementation:

  - Integrated into the product,
  - Third-party file integrity monitoring (FIM) tool.
- Integrity check of downloaded software is conducted via 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 whitelisting on the operating system which allows only known and trusted applications to be executed.

6.3 Database Integrity

Control Type: Mandatory	Applies to architecture:	A ●	B

Control Objective: Ensure the integrity of the database records for the SWIFT messaging interface.

In-scope components:

- Databases for messaging interface products

Note: this requirement is not relevant for Architecture A3 that does not have a messaging interface in the user environment.

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.

Control Context:

Database integrity checks provide a detective control against unexpected modification to records stored within the database.

Implementation Guidelines:

- Database integrity check functionality is enabled to ensure 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.

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:	A ●	B ●

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

In-scope components:

- Data exchange layer: network
- Operator PC or when used jump server: operating system
- Secure zone: connector
- Secure zone: GUI to the messaging and communication interface
- Secure zone: all server applications and operating systems
- Secure zone: network and HSM
- Secure zone: database
- Virtualisation platform (also referred as the hypervisor) hosting SWIFT-related VM’s
- [Advisory : Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT-related components]

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 store and review logs.

Control Context:

Developing a logging and monitoring plan is the basis for effectively detecting abnormal behaviour and potential attacks. 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 more straightforward logging and monitoring.

Implementation Guidelines:

- Overall goals for logging and monitoring:
  - Implement a plan for logging of security-relevant activities and configure alarms for suspicious security events (when supported by the application).
  - Implement a plan for monitoring of security events in logs and for monitoring of other data (for example, real-time business activities through the GUI), and establish a plan to treat reported alarms.
- All logging and monitoring activity complies with applicable laws and regulations, and employment contracts which supersede any implementation guidance.
- Logging:
  - Logging capabilities are implemented to detect abnormal usage within the secure zone as well as 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

Control Type: Mandatory	Applies to architecture:	A ●	B ●

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:
  - o Command line history for privileged operating system accounts on servers,
  - o Messaging and communication interface application and operating system logs which detail abnormal system behaviour (for example, activity outside normal business hours, multiple failed log-in attempts, authentication errors, changes to user groups),
  - o Firewall logs,
  - o Database logs (if available, and as a minimum in the case of hosted database solutions).

- Monitoring:
  - – Procedures are in place to identify suspicious log-in 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 either daily via human reviews or via 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.

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:	A ●	B

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

In-scope components:

- Network (data exchange layer reaching the SWIFT-related components and inside the secure zone)

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)[15] – 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 more straightforward and effective intrusion detection solutions.

Host intrusion detection systems (HIDS) are intended to protect the individual system they are implemented on in addition to detect as well as the 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 have the ability to respond to any detected intrusion (for example, terminating the connection).

Implementation Guidelines:

- 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 and/or HIDS depending on the network configuration (for instance large VLAN would better benefit of NIDS; isolated islands segregating systems may favour HIDS on those systems)
- 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 secure zone,
  - 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, an alarm is raised and, if the tool permits, a defence mechanism is triggered manually or automatically.
- Detected intrusions are managed via the standard incident response process.

Optional Enhancement:

- Intrusion detection systems have the capability to inspect encrypted flows.

Considerations for alternative implementations:

[15] Network Intrusion and Detection System

Institutions with a high level of security information and event management (SIEM) maturity within their organisation may consider extending, as per the 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:	A ●	B ●

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. Additionally, planning for the sharing of threat and incident information is critical to assisting the broader financial community in implementing effective protections against cyber attacks.

Implementation Guidelines:

- The user has developed and annually updates a cyber incident response plan. A formal backup 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) and escalation timers. Such a plan 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 and refer to SWIFT Support. Details are outlined in SWIFT-ISAC Bulletin #10047.
    - Internal security policies, laws, and regulations within a user's jurisdiction must be adhered to and considered in the cyber incident response planning.
- As a minimum, the plan is reviewed on an annual basis, and tested at least every two years ensuring safe recovery of critical business operations with minimised outage time after a cybersecurity 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 materials as may be required by SWIFT,
  - Promptly contain or isolate the impacted system to limit the exposure of the attack whilst still be able to identify rogue activities,
  - Involve skilled cybersecurity 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

Control Type: Mandatory	**Applies to architecture:**	**A** ●	**B** ●

secure operations as soon as possible,
  - Review the correctness of the user current self-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 users' jurisdiction) and to SWIFT. Sharing of threat information may potentially support root cause analysis and sharing of anonymised Indicators of Compromises (IOC) with the community.
- Information to be shared is first evaluated to ensure 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 beyond the relevance of the incident.
- The user has the capability to consume threat intelligence shared by SWIFT, for example in the form of IOCs. The user has procedures in place to:
  - Ensure the information is distributed to the correct contacts within the organisation,
  - Block traffic to/from IP-addresses/URLs mentioned in the IOCs.

Optional Enhancement:

User can integrate SWIFT ISAC TAXII API in its environment

7.2 Security Training and Awareness

Control Type: Mandatory	Applies to architecture:	A ●	B ●

Control Objective: Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.

In-scope components:

- All personnel (such as employees, agents, consultants and contractors) with access to SWIFT systems (usage, 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 including 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 appropriate knowledge and expertise.

Implementation Guidelines:

- Staff complete annual security awareness and training. Topics may include:
  - SWIFT-related products and services training (for example, via SWIFTSmart which is available to all users),
  - Cybersecurity threat awareness within the financial services industry or relevant to staff's role and responsibilities,
  - Password security and management,
  - Device security,
  - Safe operating habits (for example, spam and phishing, including “spear[16]” 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 certifications.
- Training is delivered through the most appropriate channel, including computer-based training, classroom training, webinars.
- Persons who have access to SWIFT applications, data, certificates, network, etc. have an adequate knowledge level and are aware of the pertinent cyber risks (for example, through IOCs published by SWIFT), best practice behaviours, and processes.

Optional Enhancement:

- Social engineering testing, including fake phishing emails campaign, is performed to challenge and enhance their security awareness.

[16] Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

7.3A Penetration Testing

Control Type: Advisory	Applies to architecture:	A ●	B ●

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

In-scope components:

- Operator PC or when used jump server: all hardware, software, and network
- Data exchange layer
- 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)

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 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, white box test, black box test) 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, new server or network devices, 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 component and host penetration testing (for example, rule bases and configurations review) are performed in the service production environment or in 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 TIP 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:	A ●	B ●

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)

Risk Drivers:

- Excess harm from deficient cyber readiness
- Unidentified sensitivity to cyber exposure

Implementation Guidance

Control Statement:

Scenario-driven 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 test various attacks performed by all types of unauthorised individuals on the existing systems and processes targeting the hosted SWIFT-related infrastructure. Scenario-based risk assessments are a mix of technical and business driven exercises performed as part of the institution risk management.

Such assessment considers the following non-exhaustive 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 to identify areas of risks that may require future actions, risk mitigations or update of the cyber incident response plan.

Identified actions, mitigations, or updates have to be reported and followed up for closure according to their criticality as per the Information Security Risk Management (ISRM) process.

Several ISRM frameworks exist and can be consulted (for example, on NIST, ENISA, COBRA or ISO sites or from a local or regulator's standard or controls set of the same rigour as the industry guidance) to define 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:

- A scenario 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,
  - 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 via 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/likely attacks (vectors, techniques, actors, etc.) are used as the basis for viable 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	1.4A	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
Authentication token theft																				X											
Business conducted with an unauthorised counterparty													X		X																
Compromise of enterprise authentication system	X																														
Compromise of trusted backup data									X																						
Compromise of user credentials	X																														
Credential replay	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																	
Exploitation of known security vulnerabilities						X					X												X								

SWIFT Security Controls Risk Drivers	1.1	1.2	1.3	1.4A	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
Exposure to internet-based attacks	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 of duty violations																			X												
Unauthorised access	X		X		X														X												
Unauthorised physical access																X															
Unauthorised system changes		X																						X							
Unauthenticated system traffic					X			X																							

SWIFT Security Controls **Risk Drivers**	1.1	1.2	1.3	1.4A	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
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 zone to be designed for each architecture (A1, A2, A3, B).

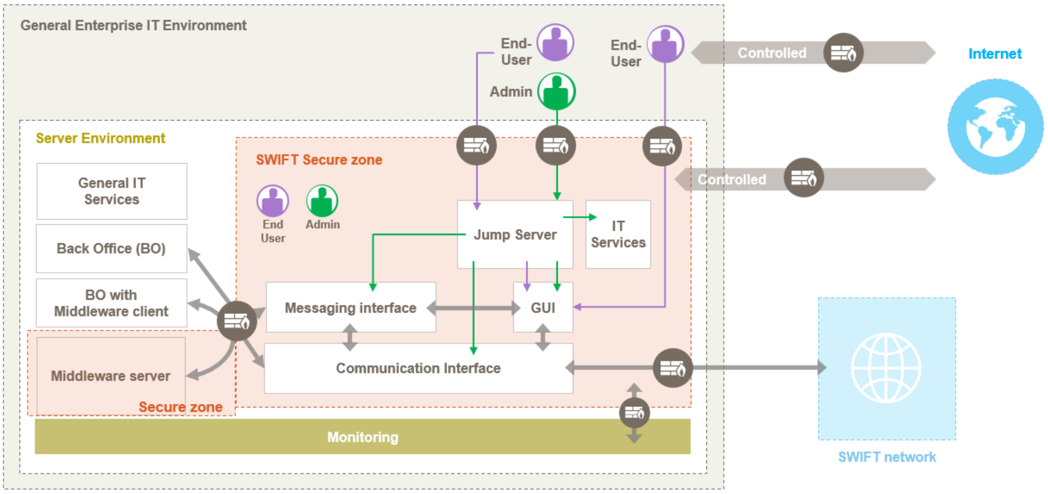

Figure 9a: Secure Zone Example for Architecture A1 - Interfaces within the user location

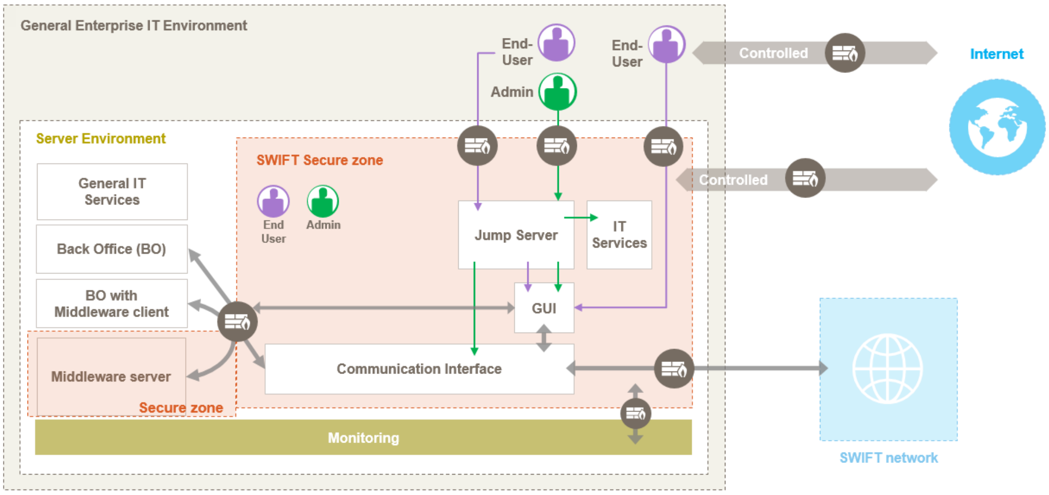

Figure 9b: Secure Zone Example for Architecture A1 - Communication interface only within the user location

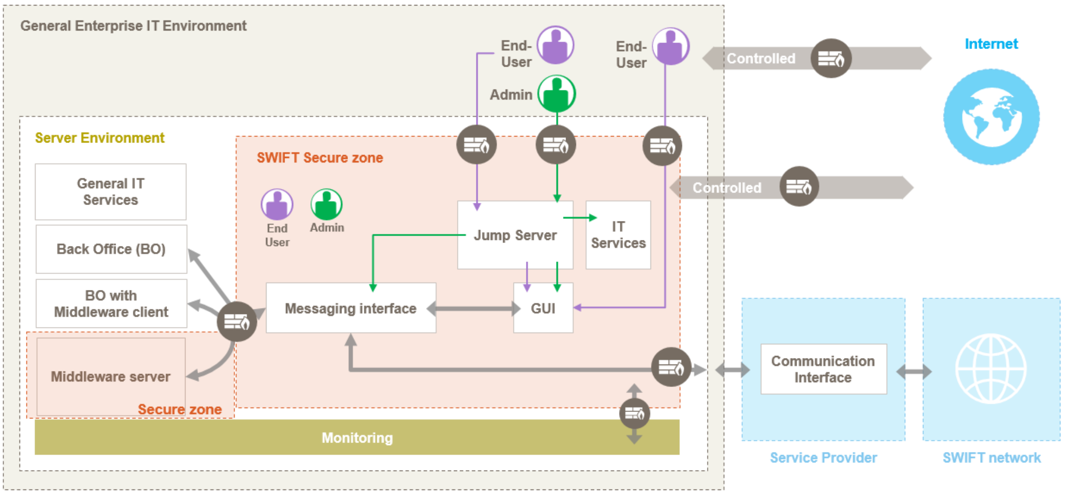

Figure 10: Secure Zone Example for Architecture A2 - Messaging interface only within the user location

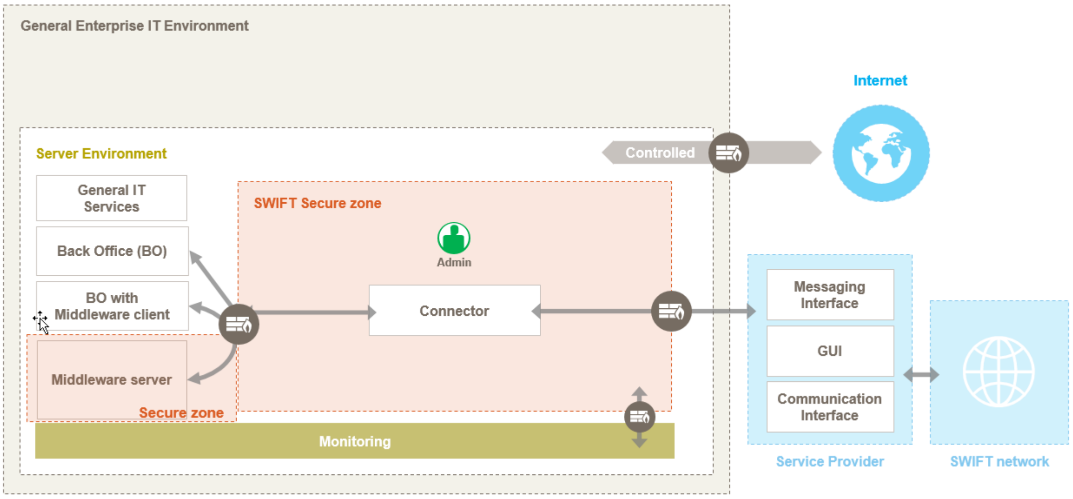

Figure 11a: Secure Zone Example for Architecture A3 - Connector

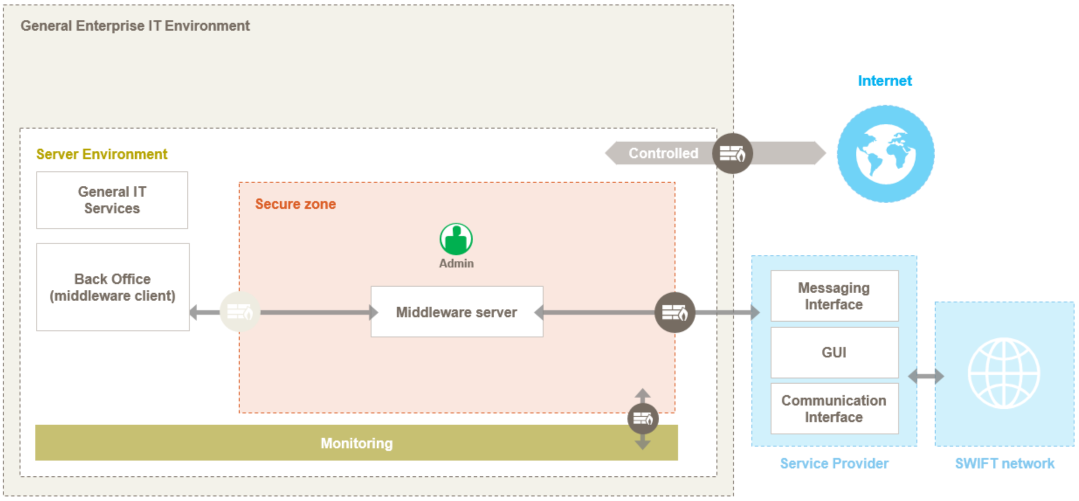

Figure 11b: Secure Zone Example for Architecture A3 – Middleware as Connector

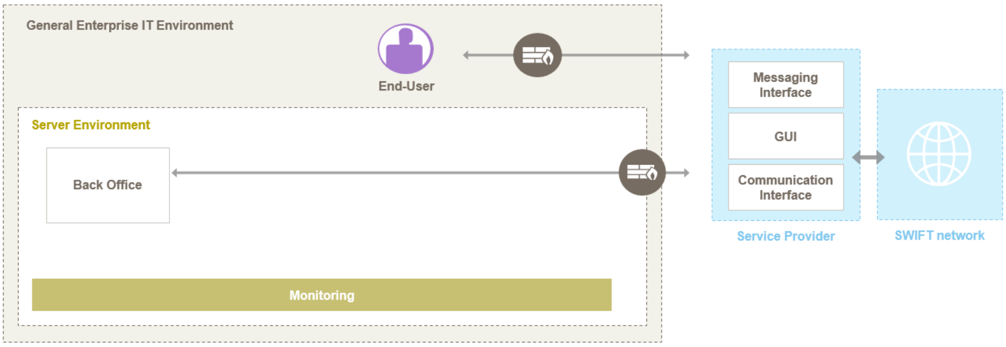

Figure 12a: Architecture B - No local footprint

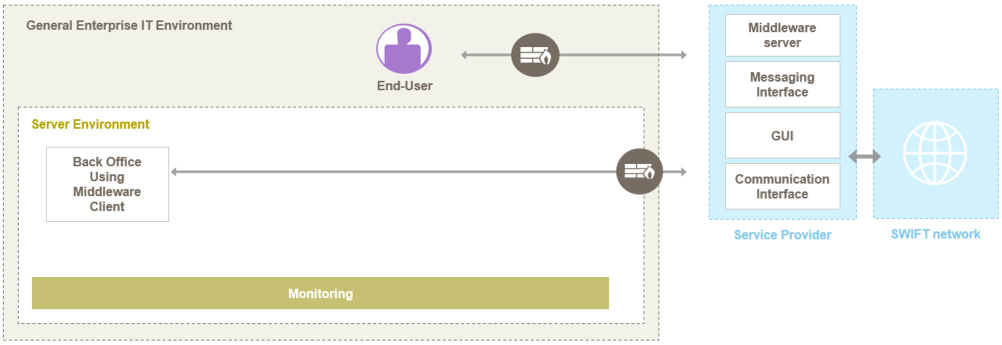

Figure 12b: Architecture B - No local footprint with middleware client

Appendix C: Sample Threat Scenarios

The following scenarios are illustrative 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 log-in credentials stored in the directory.
- Attackers compromise supporting IT infrastructure (for example, scanning server, patching server), located in the general IT environment, 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 on 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, change security configurations, 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 referred 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 or virtual machine provisioning function could create new virtual machines to further their attack, for example by creating fake application services to lure users into divulging sensitive information or download malware.
- Vulnerabilities and/or insecure configuration in the virtualisation platform may allow attackers to breach segregation between virtual machine domains.

1.4A 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 on a malicious link in an e-mail or web page, unknowingly downloading malware which compromises the local PC or server.

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.
- The operating system has aged beyond the vendor's support lifecycle 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 man-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 is able to monitor unencrypted traffic and record confidential transactions.

2.5A External Transmission Data Protection

- A data backup location is compromised, and unencrypted SWIFT backups and credential hashes are accessed, providing the attacker with valuable information about SWIFT operators and typical activity within the local environment.
- Unencrypted backups of SWIFT servers are transmitted over an insecure network connection, resulting in an adversary 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 its 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 transaction.

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 server.

2.8A Critical Activity Outsourcing

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

2.9A Transaction Business Controls

- Daily reconciliation is not performed, resulting in a fraudulent transaction going unnoticed until beyond 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 may be used by attackers to gain unauthorised access to the application.
- Excessive privileges given to application users may 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 unvetted or dormant counterparty.

3.1 Physical Security

- Poor log retention results in the inability to fully investigate which personnel 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 personnel 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 secure zone access.

4.2 Multi-factor Authentication

- Multi-factor authentication is not implemented for application access, resulting in an adversary using a stolen password to gain full access to the SWIFT messaging interface.
- Multi-factor authentication is not implemented for access to 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 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 hardware tokens results in the inability to revoke the correct tokens after staff members leave the organisation, leading into unknown and uncontrolled residual 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 Personnel Vetting Process

- A new employee with a previous judicial record for financial fraud is not vetted before being granted operator access, resulting in an untrustworthy individual being placed in a position of trust.
- Current employees are not periodically vetted, 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 personnel 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 due to not verifying the checksum 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 hiding amongst the noise of many 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 using known methods, which could have been avoided.

7.2 Security Training and Awareness

- SWIFT operators are not trained on good security practice, resulting in staff clicking on malicious phishing email links.
- SWIFT application administrators are not trained on security awareness related to their role and thus do not detect or report suspicious activity on the SWIFT systems.
- SWIFT security officers lack knowledge related to their role and thus do not properly assign privileges for operators, allowing the bypass of the segregation 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
4-eyes principle	A security principle whereby two individuals must approve an action before it can be taken. This principle is also known as two-man rule or two-person integrity.
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 via operating systems or other direct (non front-end) access
Application account	Application accounts are defined as log-ons designated for an application. They are not meant to be used by a human or GUI 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.
Connector	Connectors are local software designed to facilitate communication with a messaging or communication interface, or both. When using a connector, interface components are offered by a service provider (for example, by a service bureau, hub infrastructure, or SWIFT). Alliance Lite2 AutoClient, Direct Link, file transfer solutions, and equivalent products are considered connector solutions.
CVSS - Common Vulnerability Scoring System	CVSS is 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.
Communication interface	Communication Interface software providing a link between the SWIFTNet network and Messaging Interface software. 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) and by certified third-party vendors.
Cybersecurity incident	Any malicious act or suspicious event that compromises, or was an attempt to compromise, a computing environment.

Term	Definition
Data exchange layer	The transport of data between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office first hop 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. The flow of data between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office first hop as seen from the SWIFT-related components.
End User	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.
General (enterprise) IT environment	The general IT infrastructure used to support the broad organisation. This includes general IT services and general purpose operator PCs.
General IT services	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)	Software that produces the graphical interface for a user (that is, Alliance Web Platform and equivalent products).
Hardware token	A USB token, smart card, or similar device.
Interactive log-in / 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).
Indicators of compromise (IOC)	Artefacts that can be observed on a network or operating system that might indicate system compromise.
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)	Local Authentication, abbreviated as LAU, 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.

Term	Definition
Messaging interface	Messaging Interface software supporting the use of SWIFT messaging services (FIN, InterAct, and FileAct). 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) and by certified third-party vendors.
Middleware	Software that enables two separate programs to interact and/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, used for data exchange between the SWIFT-related components (in the local SWIFT infrastructure or at a service provider) and the user back office first hop as seen from the SWIFT-related components.
Multi-factor authentication	Multi-Factor Authentication is a method of user authentication where at least two different components are required to authenticate a user. 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)	A network access control list refers to rules that are applied to port numbers or IP addresses for controlling traffic in and out. These lists are available on a network device.
Network devices	Components used to assist in the management, routing, and security of the network (for example, routers, switches, firewalls).
Operating system (OS) accounts	User accounts on a server or PC that are used for direct access to the operating system.
Operator	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.
PIN	Personal Identification Number - A secret number that acts like a password preventing others from gaining unauthorised access to or using a token, mobile device or card.

Term	Definition
Privileged account	An account on an operating system or application that grants elevated access beyond that of a typical user. Includes administrator accounts on operating systems, and security officer or application owner accounts on applications.
Relationship Management Application (RMA)	A filter that enables the user to limit the correspondents from which messages can be received as well as 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	Access to a computer from outside of the local network. For example, from home or from another organisation's network.
Remote log-in	Log-in to a system initiated over a network connection rather than directly from the local PC.
Secure zone	A segmented zone on user premises separated from the general enterprise. The secure zone contains SWIFT-related systems (for example, messaging interface, communication interface), and optionally other protected systems.
Server Environment	Data centre or other secured physical location hosting servers.
Service bureau	A service bureau is 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, logging in, or managing sessions or security on behalf of SWIFT users. Service bureaux are subject to the Shared Infrastructure Programme.
Service provider	An organisation that provides services to SWIFT users regarding the day-to-day operation of their SWIFT connection. The services offered typically include sharing, or operating SWIFT connectivity components, logging on, or managing sessions or security for SWIFT users. Those organisations include shared infrastructure providers (for example, service bureau, shared connectivity providers, Lite2 for Business Applications, Alliance Lite2, Alliance Remote Gateway, group hub).
Single user or safe mode	Protected mode of operation that limits the privileges of the user.
Software token	Authentication token in logical (software) form.
Staff	All personnel (such as employees, agents, consultants and contractors).
Thick client	A software program installed and executed on the local operator PC, rather than via a browser interface.
Third party	An entity independent of the SWIFT user or user's SWIFT connectivity provider. For example, an outsourced IT provider.
Transaction Authentication Number (TAN)	A type of single-use password generally used in conjunction with a standard ID and password. Initially presented in a list (table).

Term	Definition
Transport Layer Security (TLS)	A cryptographic protocol that ensures confidentiality and integrity on the network and protects against replay attacks.
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 cybersecurity 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 their 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 Appendix A: Framework Core of their Cybersecurity Framework v1.1 to navigate from the following table.

Important Note:

Note that 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 its compliance with one of these industry standards is suitable to assess its 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 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 & 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 Restrict 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
2.1 Internal Data Flow Security Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.	**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 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, analyze and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. 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 back office (or middleware) applications and connecting SWIFT infrastructure 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
2.5A. 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 connecting to the local SWIFT infrastructure.	**Data Security (PR.DS)** **PR.DS-2:** Data-in-transit is protected	**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):** 8.1
2.7. Vulnerability Scanning Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.	**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, analyze and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. 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 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 & 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
2.9A. Transaction Business Controls Restrict transaction 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 using SWIFT-certified messaging and communication interfaces and 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 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, 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 authorized 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 systems, 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 (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., 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 segregation 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 hardware authentication tokens (if 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. Personnel Vetting Process Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., 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 recorded passwords.	**Access Control (PR.AC)** **PR.AC-1:** Identities and credentials are managed for authorized 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 local SWIFT infrastructure is protected against malware.	**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 applications.	**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.	**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 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 security training and awareness activities.	**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, analyze and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. 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 prioritized	**ISO 27001 Section 8.2**	**Requirement 12:** Maintain a policy that addresses information security for all personnel **Applicable Subsection(s):** 12.2

Legal Notices

Copyright

Confidentiality

This publication contains SWIFT or third-party confidential information. You must only disclose the information in this publication to your employees, agents, subcontractors, or professional advisors (or, for SWIFT users only, those persons of your affiliated entities) on a “need-to- know” basis. Do not further disclose the information in this publication without the prior written consent of SWIFT.

Translations

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

Disclaimer

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

Trademarks

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