Mapping Security Controls against Security Guidance Recommendations

19 June 2019

Introduction

“SWIFT’s Customer Security Controls Framework” (published in August 2018) details a set of 29 security controls to help SWIFT users secure their local SWIFT environment. 19 of these 29 security controls are mandatory and establish a security baseline for the entire community. The remaining 11 controls are advisory and based on good practice that SWIFT recommends users implement in their local environments. Advisory control numbers are suffixed by the letter 'A'.

Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

Note: The scope of the framework is the local SWIFT environment. However, they reflect good security practice and it is appropriate to implement them beyond the in-scope environment into the broader end-to-end transaction chain.

The table below maps each security control (product-agnostic) from the “SWIFT Customer Security Controls Framework” against related recommendations (product-specific) from the different SWIFT security guidance documents. The paragraphs titled ‘Complementary requirements’ highlight aspects from the security controls that are new requirements complementing the existing security recommendations. These new requirements and the new features or enhancements introduced in the Release 7.3 and 7.4 will be specifically included in future versions of the product-specific security guidance documents.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
1.1 SWIFT Environment Protection Control: A segregated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.11 (jump server) 4.2.4 Operating System Hardening Applicable control: OSH.02 (only software to operate, monitor and secure Alliance products) **4.3 Secure Local Client Environment** 4.3.3 Internet Access Applicable control: CIA.01 (block internet access) *Note: In the CSCF, restricted internet access is accepted, providing that:* - *Any required Internet access is permitted only if initiated in the outbound direction.* - *Internet access is only granted to whitelisted URL destinations (for example, site for downloading security patches) via a proxy with content inspection and adequate blocking/filtering controls. General browsing is not permitted.* **4.5 Local Network Security** 4.5.1 Connectivity Applicable control: CON.01 (protection against DoS attacks) 4.5.2 Network Segregation	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.11 4.2.4 Operating System Hardening Applicable control: OSH.02 **4.3 Secure Local Client Environment** 4.3.3 Internet Access Applicable control: CIA.01 4.3.6 Secure Browsing Applicable control: SBR.01 **4.5 Local Network Security** 4.5.1 Connectivity Applicable control: CON.01 4.5.2 Network Segregation Applicable control: NET.01, NET.02, NET.03, NET.04, NET.05, NET.06, NET.07 4.5.3 Front-end Reverse Proxy Applicable control: FRP.01 *Note: In the CSCF, following network configurations requirements apply:* - *Network ACLs or host-based firewalls restrict traffic on a host-by-host basis within the secure zone.* - *Individual hardware or network-based firewalls between the components in the secure zone can optionally be used.*	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: SLA.09 3.1.4 Operating System Hardening Applicable control: OSH.02 **3.2 Secure Local Client Environment** 3.2.3 Internet Access Applicable control: CIA.02 *Note: In the CSCF, restricted internet access is accepted, providing that:* - *Any required Internet access is permitted only if initiated in the outbound direction.* - *Internet access is only granted to whitelisted URL destinations (for example, site for downloading security patches) via a proxy with content inspection and adequate blocking/filtering controls. General browsing is not permitted.* **3.2 Secure Local Client Environment** 3.2.4 Secure Browsing Applicable control: CSB.01 **3.4 Local Network Security** 3.4.1 Connectivity Applicable control: CON.01 3.4.2 Network Segregation Applicable control: NET.01, NET.02, NET.03, NET.05, NET.06, NET.07	**4.2 Secure Local Server Environment** 4.2.4 Operating System Hardening Applicable control: OSH.02 **4.3 Secure Local Client Environment** 4.3.5 Secure Browsing Applicable control: ALB.01 **4.5 Local Network Security** 4.5.1 Connectivity Applicable control: CON.01 (protection against DoS attacks) 4.5.2 Network Segregation Applicable control: ALN.01, ALN.02, ALN.03, ALN.04, ALN.05, ALN.06. **Complementary requirements[1]:** - Protections of the secure zone (boundary protection & communication between components in the secure zone). - Access to the secure zone (local operator access vs. remote operator access). - Segregation from General Enterprise IT Services. - Virtualisation.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	Applicable control: NET.01, NET.02, NET.03, NET.04, NET.05, NET.06, NET.07, NET.08 *Note: In the CSCF, following network configurations requirements apply:* - *Network ACLs or host-based firewalls restrict traffic on a host-by-host basis within the secure zone.* - *Individual hardware or network-based firewalls between the components in the secure zone can optionally be used.* **Complementary requirements:[1]** - Protections of the secure zone (boundary protection & communication between components in the secure zone). - Access to the secure zone (local operator access vs. remote operator access). - Segregation from General Enterprise IT Services. - Virtualisation.	**Complementary requirements[1]:** - Protections of the secure zone (boundary protection & communication between components in the secure zone). - Access to the secure zone (local operator access vs. remote operator access). - Segregation from General Enterprise IT Services. - Virtualisation.	*Note: In the CSCF, following network configurations requirements apply:* - *Network ACLs or host-based firewalls restrict traffic on a host-by-host basis within the secure zone.* - *Individual hardware or network-based firewalls between the components in the secure zone can optionally be used.* **Complementary requirements[1]:** - Protections of the secure zone (boundary protection & communication between components in the secure zone). - Access to the secure zone (local operator access vs. remote operator access). - Segregation from General Enterprise IT Services. - Virtualisation.	

[1] Requirements included in the SWIFT Customer Security Controls Framework that complement the existing SWIFT recommendations and which are not yet specifically addressed in the product-specific security guidance

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
1.2 Operating System Privileged Account Control **Control:** 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.	New security requirement.			**4.4 Secure Local Application Environment** 4.4.1 Logical Access Control Applicable control: ALC.05 **Complementary requirements:** - Access to administrator-level operating accounts is restricted to the maximum extent possible. - Log-in with built-in administrator-level accounts is not permitted, except to perform activities where such accounts are specifically needed or in emergency situations. Individual accounts with administrator-level privileges or accounts with the ability to escalate to administrative access are used instead. - Individual administrator-level account access and usage are logged. - Administrator-level passwords are tightly controlled with physical access controls when physically recorded.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
1.3A. Virtualisation Platform Protection **Control: Secure virtualisation platform, virtualised machines and supporting virtual infrastructure (e.g. firewalls) to the same level as physical systems.**				
2.1 Internal Data Flow Security **Control:** Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT-related application-to-application and operator-to-application data flows.	**4.4 Secure Local Application Environment** 4.4.3 Confidentiality Applicable control: LSC.01, LSC.02 4.4.4 Integrity and Authentication Applicable control: LAU.01	**4.4 Secure Local Application Environment** 4.4.3 Confidentiality Applicable control: LSC.01, LSC.02 4.4.4 Integrity and Authentication Applicable control: LSC.03, LAU.01	**3.3 Secure Local Application Environment** 3.3.3 Local Server Authentication and Confidentiality Applicable control: LSC.01, LSC.02 **Complementary requirements:** - Integrity mechanisms are implemented to protect data flows between SWIFT-related applications within the secure zone, and its link to the operator PCs (SAA- AWP SE, SAA – ARG).	New security requirement.
2.2 Security Updates **Control:** All hardware and software inside the secure zone and on operator PCs are within the support lifecycle of the vendor, have been	**4.2 Secure Local Server Environment** 4.2.5 Security Updates Applicable control: SSP.01, SSP.02 **4.3 Secure Local Client Environment** *4.3.5* Security Updates	**4.2 Secure Local Server Environment** 4.2.5 Security Updates Applicable control: SSP.01 **4.3 Secure Local Client Environment** *4.3.5* Security Updates Applicable control: CSP.01	**3.1 Secure Local Server Environment** 3.1.5 Security Patches Applicable control: SSP.01, SSP.02 **3.2 Secure Local Client Environment** *3.2.6* Security Patches Applicable control: CSP.01	**4.2 Secure Local Server Environment** 4.2.5 Security Updates Applicable control: SSP.01, SSP.02 **4.3 Secure Local Client Environment** *4.3.4* Security Updates

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
upgraded with mandatory software updates, and have had security updates promptly applied.	Applicable control: CSP.01 **Complementary requirements:** - Support availability. - Security update deployment policy based in a risk assessment process and/or recommended on the Common Vulnerability Scoring System (CVSS), Version 3.	**Complementary requirements:** - Support availability. - Security update deployment policy based in a risk assessment process and/or recommended on the Common Vulnerability Scoring system (CVSS), Version 3.	**Complementary requirements:** - Support availability. - Security update deployment policy based in a risk assessment process and/or recommended on the Common Vulnerability Scoring system (CVSS), Version 3.	Applicable control: ALU.01 **Complementary requirements:** - Support availability. - Security update deployment policy based in a risk assessment process and/or recommended on the Common Vulnerability Scoring system (CVSS), Version 3.
2.3 System Hardening **Control:** Security hardening is conducted on all in-scope components.	**4.2 Secure Local Server Environment** 4.2.4 Operating System Hardening Applicable control: OSH.01 **4.5 Local Network Security** 4.5.2 Network Segregation Applicable control: NET.01 (listeners used by Alliance products) **Complementary requirements:** - Operator PCs and supporting infrastructure within the secure zone are included in the scope. - All in-scope systems are hardened in accordance with a hardening standard/guide (vendor, industry or local) but can be overruled by application-specific	**4.2 Secure Local Server Environment** 4.2.4 Operating System Hardening Applicable control: OSH.01 **Complementary requirements:** - Operator PCs and supporting infrastructure within the secure zone are included in the scope. - All in-scope systems are hardened in accordance with a hardening standard/guide (vendor, industry or local) but can be overruled by application-specific configuration requirements to maintain a proper operational state. - Documented follow-up of the implementation deviations.	**3.1 Secure Local Server Environment** 3.1.4 Operating System Hardening Applicable control: OSH.01 **Complementary requirements:** - Operator PCs and supporting infrastructure within the secure zone are included in the scope. - All in-scope systems are hardened in accordance with a hardening standard/guide (vendor, industry or local) but can be overruled by application-specific configuration requirements to maintain a proper operational state. - Documented follow-up of the implementation deviations.	**4.2 Secure Local Server Environment** 4.2.4 Operating System Hardening Applicable control: OSH.01 **Complementary requirements:** - Operator PCs and supporting infrastructure within the secure zone are included in the scope. - All in-scope systems are hardened in accordance with a hardening standard/guide (vendor, industry or local) but can be overruled by application-specific configuration requirements to maintain a proper operational state.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	configuration requirements to maintain a proper operational state. - Documented follow-up of the implementation deviations.			- Documented follow-up of the implementation deviations.
2.4A Back-Office Data Flow Security **Control**: Confidentiality, integrity, and mutual authentication mechanisms are implemented to protect data flows between back-office (or middleware) applications and connecting SWIFT infrastructure components.	**4.4 Secure Local Application Environment** 4.4.3 Confidentiality Applicable control: *The connection between Alliance Access or Alliance Gateway and the back-office application must be encrypted. This can be achieved by solutions such as MQ encryption, SFTP, and so on.* 4.4.4 Integrity and Authentication Applicable control: LAU.02, LAU.03 **Complementary requirements:** - Mutual authentication of the data flows between back-office systems (or middleware systems) and directly connected SWIFT infrastructure components.	**4.4 Secure Local Application Environment** 4.4.3 Confidentiality Applicable control: *The connection between the customer managed interface and the back-office application must be encrypted. This can be achieved by solutions such as MQ encryption, SFTP, and so on.* 4.4.4 Integrity and Authentication Applicable control: LSC.03, LAU.01 **Complementary requirements:** - Mutual authentication of the data flows between back-office systems (or middleware systems) and directly connected SWIFT infrastructure components.	**3.3 Secure Local Application Environment** 3.3.3 Local Server Authentication and Confidentiality Applicable control: LSC.03 3.3.4 Integrity Mechanisms Applicable control: LAU.01, LAU.02 **Complementary requirements:** - Mutual authentication of the data flows between back-office systems (or middleware systems) and directly connected SWIFT infrastructure components.	**4.4 Secure Local Application Environment** 4.4.2 Confidentiality, Integrity, and Authentication Applicable control: ALI.01, ALI.02, ALI.03 **Complementary requirements:** - Mutual authentication of the data flows between back-office systems (or middleware systems) and directly connected SWIFT infrastructure components.
2.5A. External Transmission Data Protection **Control:** Sensitive SWIFT-related data leaving the secure zone is encrypted.	New security requirement.			

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
2.6. Operator Session Confidentiality and Integrity **Control:** The confidentiality and integrity of interactive operator sessions connecting into the secure zone is safeguarded.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.03, SLA.10 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.03, CLA.04 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: LOA.01,AGW.01 **Complementary requirements:** - Enhanced the scope (sessions to SWIFT-related applications & OS). - All interactive sessions are protected by a cryptographic protocol (for example, ssh, https).	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.03, SLA.10 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.03, CLA.04 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: USM.03, USM.04 **Complementary requirements:** - Enhanced the scope (sessions to SWIFT-related applications & OS). - All interactive sessions are protected by a cryptographic protocol (for example, ssh, https).	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: SLA.08 **3.2 Secure Local Client Environment** 3.2.2 Logical Access Control Applicable control: CLA.03 **Complementary requirements:** - Enhanced the scope (sessions to SWIFT-related applications & OS). - All interactive sessions are protected by a cryptographic protocol (for example, ssh, https).	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.03 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: ALL.02 **Complementary requirements:** - Enhanced the scope (sessions to SWIFT-related applications & OS). - All interactive sessions are protected by a cryptographic protocol (for example, ssh, https).
2.7. Vulnerability Scanning **Control:** Secure zone and operator PC systems are scanned for	New security requirement.			

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
vulnerabilities using an up-to-date, reputable scanning tool.				
2.8A Critical Activity Outsourcing **Control**: Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.	New security requirement.			
2.9A. Transaction Business Controls **Control:** Implement RMA controls and transaction detection, prevention and validation controls to restrict transaction activity to within the expected bounds or normal business.	**4.4 Secure Local Application Environment** 4.4.5 Relationship Management Application (RMA) Applicable control: RMA.01, RMA.02, RMA.03 **4.6 Other Security Recommendations** 4.6.1 Detection Mechanisms (Reconciliation and Abnormal Sessions and message Flows) Applicable control: REC.01, ASM.01 **Complementary requirements:** - Restriction of the transactions and active SWIFTNet FIN	**4.4 Secure Local Application Environment** 4.4.5 Relationship Management Application (RMA) Applicable control: RMA.01, RMA.02, RMA.03 **4.6 Other Security Recommendations** 4.6.1 Detection Mechanisms (Reconciliation and Abnormal Sessions and message Flows) Applicable control: REC.01, ASM.01 **Complementary requirements:** - Restriction of the transactions and active SWIFTNet FIN	**3.5 Other Security Recommendations** 3.5.1 Reconciliation Applicable control: REC.01 **Complementary requirements:** - Relationship Management Application (RMA). - Restriction of the transactions and active SWIFTNet FIN sessions outside of normal business hours. - Have a process in place to issue and check confirmation messages. - Monitor uncharacteristic transactions.	**4.6 Other Security Recommendations** 4.6.1 Relationship Management Application (RMA) Applicable control: RMA.01, RMA.02, RMA.03 4.6.2.1 Reconciliation Applicable control: REC.01 4.6.2.2 Abnormal Sessions and Message Flows Applicable control: ASM.01 **Complementary requirements:** - Have a process in place to issue and check confirmation messages.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	sessions outside of normal business hours. - Have a process in place to issue and check confirmation messages. - Monitor uncharacteristic transactions.	sessions outside of normal business hours. - Have a process in place to issue and check confirmation messages. - Monitor uncharacteristic transactions.		- Monitor uncharacteristic transactions.
2.10A. Application Hardening **Control: All messaging interfaces (for example, Alliance Access, Alliance Messaging Hub and equivalent) and communication interfaces (for example, Alliance Gateway and equivalent) products within the secure zone are SWIFT-certified. Security hardening is conducted and maintained on all in-scope components.**	**This control consists for users of the SWIFT Alliance Access to comply with the Alliance Security Guideline.**	**This control consists for users of a certified messaging interface to comply with the Alliance Security Guideline.**	**This control consists for users of the Alliance Remote Gateway to comply with the Alliance Security Guideline.**	**This control consists for users of the Alliance Lite2 to comply with the Alliance Security Guideline.**
3.1. Physical Security **Control:** Physical security controls are in place to protect access to	**4.2 Secure Local Server Environment** 4.2.1 Physical Access Control Applicable control: SPA.01, SPA.02, SPA.03, SPA.04	**4.2 Secure Local Server Environment** 4.2.1 Physical Access Control Applicable control: SPA.01, SPA.02, SPA.03, SPA.04 **4.3 Secure Local Client Environment**	**3.1 Secure Local Server Environment** 3.1.1 Physical Access Control Applicable control: SPA.01, SPA.02, SPA.03, **3.2 Secure Local Client Environment**	**4.2 Secure Local Server Environment** 4.2.1 Physical Access Control Applicable control: ALS.01, ALS.02, ALS.03, ALS.04

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
sensitive equipment, hosting sites, and storage.	**4.3 Secure Local Client Environment** 4.3.1 Physical Access Control Applicable control: CPS.01 **4.4 Secure Local Application Environment** 4.4.6 Hardware Security Module Applicable control: HSM.01, HSM.02, HSM.03, HSM.04, HSM.05, HSM.06 **Complementary requirements:** - Security of the Workplace Environment. - Security for Remote Workers (for example, teleworkers, "on call" duties). - Additional requirements on the security of the Server Environment.	4.3.1 Physical Access Control Applicable control: CPS.01 **4.4 Secure Local Application Environment** 4.4.5 Hardware Security Module Applicable control: HSM.01, HSM.02, HSM.03, HSM.04, HSM.05, HSM.06 **Complementary requirements:** - Security of the Workplace Environment. - Security for Remote Workers (for example, teleworkers, "on call" duties). - Additional requirements on the security of the Server Environment.	3.1.1 Physical Access Control Applicable control: CPS.01 **3.3 Secure Local Application Environment** 3.3.5 PKI-based Security Applicable control: PKI.01, PKI.02 **Complementary requirements:** - Security of the Workplace Environment. - Security for Remote Workers (for example, teleworkers, "on call" duties). - Additional requirements on the security of the Server Environment.	**4.3 Secure Local Client Environment** 4.3.1 Physical Access Control Applicable control: ALP.01 **4.4 Secure Local Application Environment** 4.4.3 USB Token Applicable control: ALT.01, ALT.02 4.4.4 Channel Certificate Applicable control: ACC.02 **Complementary requirements:** - Security of the Workplace Environment. - Security for Remote Workers (for example, teleworkers, "on call" duties). - Additional requirements on the security of the Server Environment.
4.1 Password Policy **Control:** All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and	**4.1 SWIFT Security Governance** 4.1.1.1 SWIFTNet Security Officers Applicable controls: CAD.03 4.1.1.3 swift.com Administrators Applicable controls: SCA.06 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control	**4.1 SWIFT Security Governance** 4.1.1.1 SWIFTNet Security Officers Applicable controls: CAD.03 4.1.1.3 swift.com Administrators Applicable controls: SCA.05 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.07	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: SLA.05 **3.2 Secure Local Client Environment** 3.2.2 Logical Access Control Applicable control: CLA.01	**4.1 SWIFT Security Governance for Customers** 4.1.3 swift.com Administrators Applicable controls: SCA.05 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.07

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
the number of failed log-in attempts.	Applicable control: SLA.07 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.01 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: LOA.02, LOA.03, LOA.04, AGW.02, USM.01 **Complementary requirements:** - Password policy established and aligned to current industry standards or industry best practices and defines specified criteria. Good practice guidelines provided in the TIP 5021567. - Password policy developed in consideration of known password-based vulnerabilities in the computing environment (*that is, LAN Manage password hash*). - Effectiveness of the password policy is reviewed at least annually.	**4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.01 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: USM.01 **Complementary requirements:** - Password policy established and aligned to current industry standards or industry best practices and defines specified criteria. Good practice guidelines provided in the TIP 5021567. - Password policy developed in consideration to of known password-based vulnerabilities in the computing environment (*that is, LAN Manager password hash*). - Effectiveness of the password policy is reviewed at least annually. - Passwords for secure zone systems are stored only within the zone as described in the guidance for the design of the secure zone.	**3.3 Secure Local Application Environment** 3.3.1 Local Operator Authentication and Session Management Applicable control: USM.01 **Complementary requirements:** - Password policy established and aligned to current industry standards or industry best practices and defines specified criteria. Good practice guidelines provided in the TIP 5021567. - Password policy developed in consideration to of known password-based vulnerabilities in the computing environment (*that is, LAN Manager password hash*). - Effectiveness of the password policy is reviewed at least annually. - Passwords for secure zone systems are stored only within the zone as described in the guidance for the design of the secure zone.	**4.4 Secure Local Application Environment** 4.4.3 USB Token Applicable control: ALT.04 4.4.4 Channel Certificate Applicable control: ACC.01 **Complementary requirements:** - Password policy established and aligned to current industry standards or industry best practices and defines specified criteria. Good practice guidelines provided in the TIP 5021567. - Password policy developed in consideration to of known password-based vulnerabilities in the computing environment (*that is, LAN Manager password hash*). - Effectiveness of the password policy is reviewed at least annually. - Passwords for secure zone systems are stored only within the zone as described in the guidance for the design of the secure zone.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	- Passwords for secure zone systems are stored only within the zone as described in the guidance for the design of the secure zone.			
4.2. Multi-factor Authentication **Control:** Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.04 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: USM.02 **Complementary requirements:** - Multi-factor authentication with Operator PC and to jump server. - Prioritised order for implementing multi-factor authentication for OS admin and end-users. - Multi-factor authentication implemented for remote user administrative access	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.04 **4.4 Secure Local Application Environment** 4.4.1 Local Operator Authentication and Session Management Applicable control: USM.02 **Complementary requirements:** - Multi-factor authentication with Operator PC and to jump server. - Prioritised order for implementing multi-factor authentication for OS admin and end-users. - Multi-factor authentication implemented for remote user administrative access.	**3.3 Secure Local Application Environment** 3.3.1 Local Operator Authentication and Session Management Applicable control: USM.02 **Complementary requirements:** - Multi-factor authentication with Operator PC and to jump server. - Prioritised order for implementing multi-factor authentication for OS admin and end-users. - Multi-factor authentication implemented for remote user administrative access.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.04 **Complementary requirements:** - Multi-factor authentication with Operator PC. - Prioritised order for implementing multi-factor authentication for OS admin and end-users. - Multi-factor authentication implemented for remote user administrative access.
5.1. Logical Access Control	**4.1 SWIFT Security Governance** 4.1.1 .1 SWIFTNet Security Officers	**4.1 SWIFT Security Governance** 4.1.1 .1 SWIFTNet Security Officers	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control	**4.1 SWIFT Security Governance for Customers**

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
Control: Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties.	Applicable controls: SSO.01, SSO.02, SSO.03, SSO.04, SSO.05, CAD.01, CAD.02, CAD.04 4.1.1.2 Alliance Security Officers Applicable controls: ASO.01. ASO.02, ASO.03, ASO.04 4.1.1.3 swift.com Administrators Applicable controls: SCA.01, SCA.02, SAC.03, SCA.04, SCA.05, SCA.07 4.1.1.4 Business Officers Applicable Control: SBO.01 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.08, SLA.09 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.02 **4.4 Secure Local Application Environment** 4.4.2 Authorisation Schemes Applicable control: AAS.01, AAS.02, AAS.03, AAS.04, AAS.05, AAS.06, AAS.07, AAS.08 4.4.6 Hardware Security Module Applicable control: HSM.08, HSM.09	Applicable controls: SSO.01, SSO.02, SSO.03, SSO.04, SSO.05, CAD.01, CAD.02, CAD.04 4.1.1.2 Customer Managed Interface Security Officers Applicable controls: ASO.02, ASO.03, ASO.04 4.1.1.3 swift.com Administrators Applicable controls: SCA.01, SCA.02, SAC.03, SCA.04, SCA.06 4.1.1.4 Business Officers Applicable Control: SBO.01 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.08, SLA.09 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.02 **4.4 Secure Local Application Environment** 4.4.2 Authorisation Schemes Applicable control: AAS.01, AAS.02, AAS.03, AAS.04, AAS.05, AAS.06, AAS.07 4.4.6 Hardware Security Module Applicable control: HSM.08, HSM.09	Applicable control: SLA.04, SLA.06, SLA.07 **3.2 Secure Local Client Environment** 3.2.2 Logical Access Control Applicable control: CLA.02 **3.3 Secure Local Application Environment** 3.3.2 Authorisation Schemes Applicable control: AAS.01, AAS.02, AAS.03	4.1.1 Alliance Lite2 Customer Security Officer Applicable controls: ALG.01, ALG.02, ALG.03, ALG.04, ALQ.01, ALQ.02, ALQ.03 4.1.3 swift.com Administrators Applicable controls: SCA.01, SCA.02, SCA.03, SCA.04, SCA.06 **4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.08 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: ALL.01 **4.4 Secure Local Application Environment** 4.4.1 Logical Access Control Applicable control: ALC.01, ALC.02, ALC.03, ALC.04, ALC.05, ALC.06

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
5.2. Token Management Control: Connected hardware authentication tokens are managed appropriately during issuance, revocation, use, and storage.	**4.4 Secure Local Application Environment** 4.4.6 Hardware Security Module Applicable control: HSM.07 **Complementary requirements:** - Enhanced the scope (*connected hardware authentication tokens used for SWIFT operations*). - A record is maintained of hardware token ownership.	**4.4 Secure Local Application Environment** 4.4.6 Hardware Security Module Applicable control: HSM.01, HSM.02, HSM.03, HSM.04, HSM.05, HSM.06, HSM.07 **Complementary requirements:** - Enhanced the scope (*connected hardware authentication tokens used for SWIFT operations*) - A record is maintained of hardware token ownership.	**3.3 Secure Local Application Environment** 3.3.5 PKI-based Security Applicable control: PKI.01, PKI.03 **Complementary requirements:** - Enhanced the scope (*connected hardware authentication tokens used for SWIFT operations*) - A record is maintained of hardware token ownership.	**4.4 Secure Local Application Environment** 4.4.3 USB Token Applicable control: ALT.03 **Complementary requirements:** - A record is maintained of hardware token ownership.
5.3A. Personnel Vetting Process **Control:** Staff operating the local SWIFT infrastructure are vetted prior to initial employment in that role and periodically thereafter.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.01 **Complementary requirements:** - Personnel Vetting Process.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.01 **Complementary requirements:** - Personnel Vetting Process.	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: SLA.01 **Complementary requirements:** - Personnel Vetting Process.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.01 **Complementary requirements:** - Personnel Vetting Process.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
5.4. Physical and Logical Password Storage **Control:** Any recorded passwords for privileged accounts are stored in a protected physical or logical location, with access restricted on a need-to-know basis.	New security requirement.			
6.1. Malware Protection **Control:** Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.	**4.2 Secure Local Server Environment** 4.2.6 Security Software Applicable control: IDS.01 **4.3 Secure Local Client Environment** 4.3.4 Anti-virus and Anti-malware Services Applicable control: CAV.01 **Complementary requirements:** - Anti-malware software from a reputable vendor is installed on all computing platforms and updated daily. - 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.	**4.2 Secure Local Server Environment** 4.2.6 Security Software Applicable control: IDS.01, IDS.02 **4.3 Secure Local Client Environment** 4.3.4 Anti-virus and Anti-malware Services Applicable control: CAV.01 **Complementary requirements:** - Anti-malware software from a reputable vendor is installed on all computing platforms and updated daily. - 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.	**3.1 Secure Local Server Environment** 3.1.6 Security Software Applicable control: IDS.01 **3.2 Secure Local Client Environment** 3.2.5 Anti-virus and Anti-malware Services Applicable control: CAV.01 **Complementary requirements:** - Anti-malware software from a reputable vendor is installed on all computing platforms and updated daily. - 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.	**4.2 Secure Local Server Environment** 4.2.6 Security Software Applicable control: IDS.01 **4.3 Secure Local Client Environment** 4.3.3 Anti-virus and Anti-malware Services Applicable control: ALM.01 **Complementary requirements:** - Anti-malware software from a reputable vendor is installed on all computing platforms and updated daily.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
6.2 Software Integrity Control: A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications.	**4.4 Secure Local Application Environment** 4.4.4 Integrity and Authentication Applicable control: SWI.01, SWI.02, SWI.03 **Complementary requirements:** - Scope enlarged with stand-alone RMA application and SNL.	**4.4 Secure Local Application Environment** 4.4.4 Integrity and Authentication Applicable control: SWI.01, SWI.03 **Complementary requirements:** - Scope enlarged with stand-alone RMA application and SNL.	**3.3 Secure Local Application Environment** 3.3.4 Integrity Mechanisms Applicable control: SWI.01, SWI.02, SWI.03	New security requirement.
6.3 Database Integrity **Control:** A database integrity check is performed at regular intervals on databases that record SWIFT transactions.	**4.4 Secure Local Application Environment** 4.4.4 Integrity and Authentication Applicable control: DBI.01	**4.4 Secure Local Application Environment** 4.4.4 Integrity and Authentication Applicable control: DBI.01	**3.3 Secure Local Application Environment** 3.3.4 Integrity Mechanisms Applicable control: DBI.01	Not applicable.
6.4 Logging and Monitoring **Control:** Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.06, SLA.12 4.2.3 Operating System Activity Logging Applicable control: SLG.01, SLG.02, SLG.03, SLG.04 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.06, SLA.12 4.2.3 Operating System Activity Logging Applicable control: SLG.01, SLG.02, SLG.03, SLG.04 **4.3 Secure Local Client Environment** 4.3.2 Logical Access Control Applicable control: CLA.05	**3.1 Secure Local Server Environment** 3.1.3 Operating System Activity Logging Applicable control: SLG.01, SLG.02, SLG.03, SLG.04 **3.3 Secure Local Application Environment** 3.3. Auditing and Monitoring Applicable control: ALG.01, ALG.02, ALG.03, ALG.04	**4.1 SWIFT Security Governance for Customers** 4.1.1 Alliance Lite2 Customer Security Officer Applicable controls: ALQ.04, ALQ.05 **4.2 Secure Local Server Environment** 4.2.3 Operating System Activity Logging

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	Applicable control: CLA.05 **4.4 Secure Local Application Environment** 4.4.2 Authorisation Schemes Applicable control: AAS.07, 4.4.8 Auditing and Monitoring Applicable control: ALG.01, ALG.02, ALG.03, ALG.04, ALG.05 **4.5 Local Network Security** 4.5.2 Network Segregation Applicable control: NET.09 **Complementary requirements:** - Enhanced the scope (*data exchange layer:network, database, all server applications and OS*). - Retention period of audit logs. - Types of log files to collect and monitor.	**4.4 Secure Local Application Environment** 4.4.8 Auditing and Monitoring Applicable control: ALG.01, ALG.02, ALG.03, ALG.04, ALG.05 **4.5 Local Network Security** 4.5.2 Network Segregation Applicable control: NET.08 **Complementary requirements:** - Enhanced the scope (*data exchange layer:network, database, all server applications and OS*). - Retention period of the audit logs. - Types of log files to collect and monitor.	**3.4 Local Network Security** 3.4.2 Network Segregation Applicable control: NET.08 **Complementary requirements:** - Enhanced the scope (*data exchange layer:network, database, all server applications and OS*). - Retention period of the audit logs. - Types of log files to collect and monitor.	Applicable control: SLG.01, SLG.02, SLG.03, SLG.04 **4.4 Secure Local Application Environment** 4.4.5 Auditing and Monitoring Applicable control: ALA.01, ALA.02, ALA.03 **4.5 Local Network Security** 4.5.2 Network Segregation Applicable control: ALN.07 **Complementary requirements:** - Enhanced the scope (*data exchange layer:network, database, all server applications and OS*). - Retention period of the audit logs. - Types of log files to collect and monitor.
6.5A Intrusion Detection **Control:** Intrusion detection is implemented to detect unauthorised network access and anomalous activity.	**4.5 Local Network Security** 4.5.4 Network Intrusion Detection Systems Applicable control: NID.01	**4.5 Local Network Security** 4.5.4 Network Intrusion Detection Systems Applicable control: NID.01	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: IDS.01	**4.2 Secure Local Server Environment** 4.2.6 Security Software Applicable control: IDS.01

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
7.1. Cyber Incident Response Planning Control: The organisation has a defined and tested cyber incident response plan.	**4.6 Other Security Recommendations** 4.6.2 Backup and Resilience Applicable control: SBS.01, SBS.02, SBS.03 4.6.4 Incident Management Applicable control: IMA.01, IMA.02 **Complementary requirements:** - The organisation has a defined cyber incident response plan which is reviewed on annual basis, and tested at least every two years. - Provided steps to be included in the plan in case of cyber incidents that compromise the confidentiality, integrity, or availability of SWIFT services and products. - The organisation has a documented plan for the timely sharing of threat information to intelligence-sharing organisations, law enforcement/local regulators	**4.6 Other Security Recommendations** 4.6.2 Backup and Resilience Applicable control: SBS.01, SBS.02, SBS.03 4.6.4 Incident Management Applicable control: IMA.01, IMA.02 **Complementary requirements:** - The organisation has a defined cyber incident response plan which is reviewed on annual basis, and tested at least every two year. - Provided steps to be included in the plan in case of cyber incidents that compromise the confidentiality, integrity, or availability of SWIFT services and products. - The organisation has a documented plan for the timely sharing of threat information to intelligence-sharing organisations, law enforcement/local regulators	**3.5 Other Security Recommendations** 3.5.2 Backup and Resilience Applicable control: SBS.01, SBS.02, SBS.03 3.5.4 Incident Management Applicable control: IMA.01, IMA.02 **Complementary requirements:** - The organisation has a defined cyber incident response plan which is reviewed on annual basis, and tested at least every two year. - Provided steps to be included in the plan in case of cyber incidents that compromise the confidentiality, integrity, or availability of SWIFT services and products. - The organisation has a documented plan for the timely sharing of threat information to intelligence-sharing organisations, law enforcement/local regulators	**4.6 Other Security Recommendations** 4.6.3 Resilience and Backup Applicable control: SBS.01, SBS.03 4.6.5 Incident Management Applicable control: IMA.01, IMA.02 **Complementary requirements:** - The organisation has a defined cyber incident response plan which is reviewed on annual basis, and tested at least every two year. - Provided steps to be included in the plan in case of cyber incidents that compromise the confidentiality, integrity, or availability of SWIFT services and products. - The organisation has a documented plan for the timely sharing of threat

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
	(as required in each customers' jurisdiction), and to SWIFT. - The organisation has the capability to consume threat intelligence shared by SWIFT.	(as required in each customers' jurisdiction), and to SWIFT. - The organisation has the capability to consume threat intelligence shared by SWIFT.	(as required in each customers' jurisdiction), and to SWIFT. - The organisation has the capability to consume threat intelligence shared by SWIFT.	information to intelligence-sharing organisations, law enforcement/local regulators (as required in each customers' jurisdiction), and to SWIFT. - The organisation has the capability to consume threat intelligence shared by SWIFT.
7.2. Security Training and Awareness Control: Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.02, SLA.05 **4.6 Other Security Recommendations** 4.6.3 User Security Awareness Applicable control: UAW.01 **Complementary requirements:** - Frequency of the training and security awareness sessions.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.02, SLA.05 **4.3 Secure Local Client Environment** 4.3.6 Secure Browsing Applicable control: SBR.02, SBR.03 **4.6 Other Security Recommendations** 4.6.3 User Security Awareness Applicable control: UAW.01 **Complementary requirements:** - Frequency of the training and security awareness sessions.	**3.1 Secure Local Server Environment** 3.1.2 Logical Access Control Applicable control: SLA.02, SLA.03 **3.2 Secure Local Client Environment** 3.2.4 Secure Browsing Applicable control: CSB.01 **3.5 Other Security Recommendations** 3.5.3 User Security Awareness Applicable control: UAW.01 **Complementary requirements:** - Frequency of the training and security awareness sessions.	**4.2 Secure Local Server Environment** 4.2.2 Logical Access Control Applicable control: SLA.02, SLA.05 **4.3 Secure Local Client Environment** 4.3.5 Secure Browsing Applicable control: ALB.01 **4.6 Other Security Recommendations** 4.6.4 User Security Awareness Applicable control: UAW.01 **Complementary requirements:** - Frequency of the training and security awareness sessions.

SWIFT Security Control	Alliance Security Guidance	Certified Customer Managed Interface Security Guidance	Alliance Remote Gateway Security Guidance	Alliance Lite2 Security Guidance
7.3A. Penetration Testing **Control:** Application, host, and network penetration testing is conducted within the secure zone and on user PCs.	New security requirement.			
7.4A. Scenario Risk Assessments **Control:** Scenario-driven risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organisation's security programme.	New security requirement.			

Legal Notices