

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

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: - 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 requirements¹: - 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 requirements¹: 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	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-
all other times, an account with least privilege access is used.				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	4.4 Secure Local Application	4.4 Secure Local Application	3.3 Secure Local Application	New security requirement.
Security	Environment	Environment	Environment	
Control: Confidentiality,	4.4.3 Confidentiality	4.4.3 Confidentiality	3.3.3 Local Server Authentication and	
integrity, and	Applicable control: LSC.01, LSC.02 4.4.4 Integrity and Authentication	Applicable control: <u>LSC.01, LSC.02</u> 4.4.4 Integrity and Authentication	Confidentiality Applicable control: <u>LSC.01, LSC.02</u>	
authentication	Applicable control: <u>LAU.01</u>	Applicable control: LSC.03, LAU.01	Applicable control. <u>LSC.01, LSC.02</u>	
mechanisms are	Applicable control: <u>LAO.01</u>	Applicable control. <u>LSC.03, LAO.01</u>		
implemented to protect			Complementary requirements:	
SWIFT-related			- Integrity mechanisms are	
application-to-application			implemented to protect data	
and operator-to-			flows between SWIFT-related	
application data flows.			applications within the secure	
			zone, and its link to the operator PCs (SAA- AWP SE, SAA – ARG).	
2.2.6	4.2 Secure Local Server	4.2 Secure Local Server Environment	3.1 Secure Local Server Environment	4.2 Secure Local Server
2.2 Security Updates	Environment	4.2.5 Security Updates	3.1.5 Security Patches	Environment
Control: All hardware and	4.2.5 Security Updates	Applicable control: <u>SSP.01</u>	Applicable control: <u>SSP.01, SSP.02</u>	4.2.5 Security Updates
software inside the	Applicable control: <u>SSP.01, SSP.02</u>			Applicable control: <u>SSP.01, SSP.02</u>
secure zone and on		4.3 Secure Local Client Environment	3.2 Secure Local Client Environment	
operator PCs are within	4.3 Secure Local Client	4.3.5 Security Updates	3.2.6 Security Patches	4.3 Secure Local Client
the support lifecycle of	Environment	Applicable control: <u>CSP.01</u>	Applicable control: <u>CSP.01</u>	Environment
the vendor, have been	4.3.5 Security Updates			4.3.4 Security Updates

ole control: <u>CSP.01</u> mentary requirements: port availability.	Complementary requirements: - Support availability.	Complementary requirements:	Applicable control: ALU.01
urity update deployment cy based in a risk essment process and/or ommended on the nmon Vulnerability Scoring eem (CVSS), Version 3.	- Security update deployment policy based in a risk assessment process and/or recommended on the Common Vulnerability Scoring system (CVSS), Version 3.	 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.
re Local Server	4.2 Secure Local Server Environment	3.1 Secure Local Server Environment	4.2 Secure Local Server
derating System Hardening ole control: OSH.01 Il Network Security of twork Segregation ole control: NET.01 Is used by Alliance of the system of the control of the contro	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.	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.	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.
	essment process and/or ommended on the nmon Vulnerability Scoring tem (CVSS), Version 3. The Local Server ment perating System Hardening ole control: OSH.01 If Network Security etwork Segregation ole control: NET.01 Is used by Alliance as used by Alliance so mentary requirements: erator PCs and supporting astructure within the cure zone are included in the ope. In-scope systems are dened in accordance with a	Scoring system (CVSS), Version 3. Scoring system (CVSS), Version 5. Scoring system (CVS), version 5. Scoring System Hardening 6. Scoring System Hard	Scoring system (CVSS), Version 3. Scoring system (CVSS), Version 5. Scoring system (CVS) 5. Scoring system (CVS) 5. Scoring Standarding 5. Scoring Standarding 6. Scoring Standarding 6.

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	New security requirement.			
operator PC systems are scanned for				

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	New security requirement.			
Control: Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation.				
2.04 Turneration	4.4 Secure Local Application	4.4 Secure Local Application	3.5 Other Security	4.6 Other Security
2.9A. Transaction Business Controls	Environment	Environment	Recommendations	Recommendations
Business Controls	4.4.5 Relationship Management	4.4.5 Relationship Management	3.5.1 Reconciliation	4.6.1 Relationship Management
Control: Implement RMA	Application (RMA)	Application (RMA)	Applicable control: REC.01	Application (RMA)
controls and transaction	Applicable control: RMA.01,	Applicable control: RMA.01, RMA.02,		Applicable control: RMA.01,
detection, prevention and	RMA.02, RMA.03	<u>RMA.03</u>	Complementary requirements:	RMA.02, RMA.03
validation controls to			- Relationship Management	4.6.2.1 Reconciliation
restrict transaction	4.6 Other Security	4.6 Other Security	Application (RMA).	Applicable control: <u>REC.01</u>
activity to within the	Recommendations	Recommendations	- Restriction of the transactions	4.6.2.2 Abnormal Sessions and
expected bounds or	4.6.1 Detection Mechanisms	4.6.1 Detection Mechanisms	and active SWIFTNet FIN	Message Flows
normal business.	(Reconciliation and Abnormal	(Reconciliation and Abnormal	sessions outside of normal	Applicable control: <u>ASM.01</u>
	Sessions and message Flows)	Sessions and message Flows)	business hours.	
	Applicable control: <u>REC.01, ASM.01</u>	Applicable control: <u>REC.01, ASM.01</u>	- Have a process in place to issue	Complementary requirements:
			and check confirmation	- Have a process in place to
	Complementary requirements:	Complementary requirements:	messages.	issue and check confirmation
	- Restriction of the transactions	- Restriction of the transactions	- Monitor uncharacteristic	messages.
	and active SWIFTNet FIN	and active SWIFTNet FIN	transactions.	

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

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-	Applicable control: SLA.07		3.3 Secure Local Application	
in attempts.		4.3 Secure Local Client Environment	Environment	4.4 Secure Local Application
·	4.3 Secure Local Client	4.3.2 Logical Access Control	3.3.1 Local Operator Authentication	Environment
	Environment	Applicable control: <u>CLA.01</u>	and Session Management	4.4.3 USB Token
	4.3.2 Logical Access Control		Applicable control: <u>USM.01</u>	Applicable control: <u>ALT.04</u>
	Applicable control: <u>CLA.01</u>	4.4 Secure Local Application		4.4.4 Channel Certificate
		Environment	Complementary requirements:	Applicable control: ACC.01
	4.4 Secure Local Application	4.4.1 Local Operator Authentication	- Password policy established and	
	Environment	and Session Management	aligned to current industry	Complementary requirements:
	4.4.1 Local Operator	Applicable control: <u>USM.01</u>	standards or industry best	- Password policy established
	Authentication and Session		practices and defines specified	and aligned to current
	Management	Complementary requirements:	criteria. Good practice guidelines	industry standards or
	Applicable control: LOA.02, LOA.03,	- Password policy established and	provided in the TIP 5021567.	industry best practices and
	LOA.04, AGW.02, USM.01	aligned to current industry	- Password policy developed in	defines specified criteria.
		standards or industry best	consideration to of known	Good practice guidelines
	Complementary requirements:	practices and defines specified	password-based vulnerabilities	provided in the TIP 5021567.
	- Password policy established	criteria. Good practice guidelines	in the computing environment	- Password policy developed in
	and aligned to current industry	provided in the TIP 5021567.	(that is, LAN Manager password	consideration to of known
	standards or industry best	- Password policy developed in	hash).	password-based
	practices and defines specified	consideration to of known	- Effectiveness of the password	vulnerabilities in the
	criteria. Good practice	password-based vulnerabilities	policy is reviewed at least	computing environment
	guidelines provided in the TIP	in the computing environment	annually.	(that is, LAN Manager
	5021567.	(that is, LAN Manager password	- Passwords for secure zone	password hash).
	- Password policy developed in	hash).	systems are stored only within	- Effectiveness of the
	consideration of known	- Effectiveness of the password	the zone as described in the	password policy is reviewed
	password-based vulnerabilities	policy is reviewed at least	guidance for the design of the	at least annually.
	in the computing environment	annually.	secure zone.	 Passwords for secure zone
	(that is, LAN Manage password	- Passwords for secure zone		systems are stored only
	hash).	systems are stored only within		within the zone as described
	- Effectiveness of the password	the zone as described in the		in the guidance for the
	policy is reviewed at least	guidance for the design of the		design of the secure zone.
	annually.	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	4.2 Secure Local Server	4.2 Secure Local Server Environment	3.3 Secure Local Application	4.2 Secure Local Server
Authentication	Environment	4.2.2 Logical Access Control	Environment	Environment
Control: Multi-factor	4.2.2 Logical Access Control	Applicable control: <u>SLA.04</u>	3.3.1 Local Operator Authentication	4.2.2 Logical Access Control
authentication is used for	Applicable control: <u>SLA.04</u>	4.4 Secure Local Application	and Session Management Applicable control: <u>USM.02</u>	Applicable control: <u>SLA.04</u>
interactive user access to	4.4 Secure Local Application	Environment	Applicable control. <u>OSWI.OZ</u>	Complementary requirements:
SWIFT-related	Environment	4.4.1 Local Operator Authentication	Complementary requirements:	- Multi-factor authentication
applications and	4.4.1 Local Operator	and Session Management	- Multi-factor authentication with	with Operator PC.
operating system	Authentication and Session	Applicable control: <u>USM.02</u>	Operator PC and to jump server.	- Prioritised order for
accounts.	Management		- Prioritised order for	implementing multi-factor
	Applicable control: <u>USM.02</u>	Complementary requirements: - Multi-factor authentication with	implementing multi-factor authentication for OS admin	authentication for OS admin and end-users.
	Complementary requirements:	Operator PC and to jump server.	and end-users.	- Multi-factor authentication
	- Multi-factor authentication	- Prioritised order for	- Multi-factor authentication	implemented for remote
	with Operator PC and to jump	implementing multi-factor	implemented for remote user	user administrative access.
	server.	authentication for OS admin	administrative access.	
	- Prioritised order for	and end-users.		
	implementing multi-factor authentication for OS admin	 Multi-factor authentication implemented for remote user 		
	and end-users.	administrative access.		
	- Multi-factor authentication	daministrative decess.		
	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	New security requirement.			
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.				
6.1. Malware Protection	4.2 Secure Local Server	4.2 Secure Local Server Environment	3.1 Secure Local Server Environment	4.2 Secure Local Server
Control: Anti-malware	Environment	4.2.6 Security Software	3.1.6 Security Software	Environment
software from a	4.2.6 Security Software Applicable control: IDS.01	Applicable control: <u>IDS.01</u> , <u>IDS.02</u>	Applicable control: <u>IDS.01</u>	4.2.6 Security Software Applicable control: IDS.01
reputable vendor is	Applicable control. <u>IDS.01</u>	4.3 Secure Local Client Environment	3.2 Secure Local Client Environment	Applicable control. <u>IDS.01</u>
installed and kept up-to-	4.3 Secure Local Client	4.3.4 Anti-virus and Anti-malware	3.2.5 Anti-virus and Anti-malware	4.3 Secure Local Client
date on all systems.	Environment	Services	Services	Environment
	4.3.4 Anti-virus and Anti-malware	Applicable control: <u>CAV.01</u>	Applicable control: CAV.01	4.3.3 Anti-virus and Anti-malware
	Services			Services
	Applicable control: <u>CAV.01</u>	Complementary requirements:	Complementary requirements:	Applicable control: <u>ALM.01</u>
	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.	 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. 	 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. 	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 standalone 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 standalone 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
		interface Security Guidance	Guidance	
	4.6.Othor Societies	A.C. Othor Sociultu	2.F. Othor Convitor	A.C.Okhor Soouviku
7.1. Cyber Incident	4.6 Other Security Recommendations	4.6 Other Security Recommendations	3.5 Other Security Recommendations	4.6 Other Security Recommendations
Response Planning	4.6.2 Backup and Resilience	4.6.2 Backup and Resilience	3.5.2 Backup and Resilience	4.6.3 Resilience and Backup
Control: The organisation	•	•		Applicable control: SBS.01,
has a defined and tested	Applicable control: <u>SBS.01</u> , <u>SBS.02</u> , SBS.03	Applicable control: <u>SBS.01, SBS.02,</u> SBS.03	Applicable control: <u>SBS.01, SBS.02,</u> SBS.03	SBS.03
cyber incident response	4.6.4 Incident Management	4.6.4 Incident Management	3.5.4 Incident Management	4.6.5 Incident Management
plan.	Applicable control: IMA.01, IMA.02	Applicable control: IMA.01, IMA.02	Applicable control: IMA.01, IMA.02	Applicable control: IMA.01,
	Applicable control. INVII.01, INVII.02	7. (pp. 100 10 10 11 11 11 11 11 11 11 11 11 11	7. Applicable control. 1141/1.02, 1141/1.02	IMA.02
	Complementary requirements:	Complementary requirements:	Complementary requirements:	<u></u>
	- The organisation has a defined	- The organisation has a defined	- The organisation has a defined	Complementary requirements:
	cyber incident response plan	cyber incident response plan	cyber incident response plan	- The organisation has a
	which is reviewed on annual	which is reviewed on annual	which is reviewed on annual	defined cyber incident
	basis, and tested at least every	basis, and tested at least every	basis, and tested at least every	response plan which is
	two years.	two year.	two year.	reviewed on annual basis,
	- Provided steps to be included	- Provided steps to be included in	- Provided steps to be included in	and tested at least every two
	in the plan in case of cyber	the plan in case of cyber	the plan in case of cyber	year.
	incidents that compromise the	incidents that compromise the	incidents that compromise the	- Provided steps to be
	confidentiality, integrity, or	confidentiality, integrity, or	confidentiality, integrity, or	included in the plan in case
	availability of SWIFT services	availability of SWIFT services	availability of SWIFT services	of cyber incidents that
	and products.	and products.	and products.	compromise the
	- The organisation has a	- The organisation has a	- The organisation has a	confidentiality, integrity, or
	documented plan for the	documented plan for the timely	documented plan for the timely	availability of SWIFT services
	timely sharing of threat	sharing of threat information to	sharing of threat information to	and products.
	information to intelligence-	intelligence-sharing	intelligence-sharing	- The organisation has a
	sharing organisations, law	organisations, law	organisations, law	documented plan for the
	enforcement/local regulators	enforcement/local regulators	enforcement/local regulators	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	4.2 Secure Local Server	4.2 Secure Local Server Environment	3.1 Secure Local Server Environment	4.2 Secure Local Server
and Awareness	Environment	4.2.2 Logical Access Control	3.1.2 Logical Access Control	Environment
Control: Annual security	4.2.2 Logical Access Control	Applicable control: <u>SLA.02</u> , <u>SLA.05</u>	Applicable control: <u>SLA.02</u> , <u>SLA.03</u>	4.2.2 Logical Access Control
awareness sessions are	Applicable control: SLA.02, SLA.05			Applicable control: <u>SLA.02</u> ,
conducted for all staff		4.3 Secure Local Client Environment	3.2 Secure Local Client Environment	<u>SLA.05</u>
members, including role-	4.6 Other Security	4.3.6 Secure Browsing	3.2.4 Secure Browsing	
specific training for SWIFT	Recommendations	Applicable control: <u>SBR.02</u> , <u>SBR.03</u>	Applicable control: <u>CSB.01</u>	4.3 Secure Local Client
•	4.6.3 User Security Awareness	4.C. Other Consuits	3.5. Other Consists	Environment
roles with privileged	Applicable control: <u>UAW.01</u>	4.6 Other Security Recommendations	3.5 Other Security Recommendations	4.3.5 Secure Browsing Applicable control: ALB.01
access.	Complementary requirements:	4.6.3 User Security Awareness	3.5.3 User Security Awareness	Applicable control: ALB.01
	- Frequency of the training and	Applicable control: <u>UAW.01</u>	Applicable control: <u>UAW.01</u>	4.6 Other Security
	security awareness sessions.	Applicable control. <u>OAW.01</u>	Applicable control. <u>GAV.01</u>	Recommendations
	security awareness sessions.	Complementary requirements:	Complementary requirements:	4.6.4 User Security Awareness
		 Frequency of the training and security awareness sessions. 	 Frequency of the training and security awareness sessions. 	Applicable control: <u>UAW.01</u>
				- 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

Copyright

SWIFT © 2019. All rights reserved.

Restricted Distribution

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

Disclaimer

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

Translations

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

Trademarks

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