SWIFT Lite2 for Business Applications Programme, Security and Operational Framework for 2021

SELF-ATTESTATION

This form should be used to submit your self-attestation of compliance towards the controls of the Lite2 for Business Applications Programme, Security and Operational Framework for 2021 (L2BASOFv2021).

The L2BASOFv2021 becomes effective on the 1st of January 2021, and all providers will need to be full compliant by the 31st of December 2021. **All (applicable) controls are mandatory.**

L2BA Providers may be published as qualified against 2021 requirements after having uploaded a self-attestation declaring full compliance to the applicable controls.

CONTACT DETAILS

Service Bureau	
BIC*	

Contact Person for Self-Attestation	
First name or department name*	
Last Name (in case of a person)*	
Job Title (in case of a person)	
Direct Work Phone*	
E-mail address*	

CISO or similar role	
First name*	
Last Name*	
Job Title	
Direct Work Phone*	
Phone number in case of emergencies*	
E-mail address*	

Contact Person #1 of the 24x7 SOC	
First name or department name*	
Last Name (in case of a person)*	
Job Title (in case of a person)	
Direct Work Phone*	
Phone number in case of emergencies*	
E-mail address*	

Contact Person #2 of the 24x7 SOC	
First name	
Last Name	
Job Title	
Direct Work Phone	
Phone number in case of emergencies	
E-mail address	

* Mandatory fields

SELF ATTESTATION – L2BASOFV2021

L2BA Provider BIC	
I have read the CSCF document	☐
I have read the L2BASOF document	☐
Target date for full compliance against L2BASOFv2021 (DD-MMM-YY)	

Controls in rows with white background are related to the control requirements defined in the Customer Security Controls Framework v2021 (CSCFv2021) from SWIFT Customer Security Program (CSP).
Controls in rows with grey background are related to the control requirements defined in the L2BASOFv2021.

How to answer?
Select from the drop down menu in the column 'Compliance' your current 'Compliance level' for all the listed controls taking into account the implementation guidelines detailed in the CSCF (white controls) or in the L2BASOF (grey controls).

Once the form has been filled in, please request a SWIFT Post upload link to SB.certification.office@swift.com.

Note, when you are in the process of applying changes that affect a control compliance status:
– Assess current implementation
– Once the new implementation is effective, resubmit the self attestion with the changed compliance level

CONTROL OBJECTIVE: SECURE YOUR ENVIRONMENT
CONTROL PRINCIPLE: RESTRICT INTERNET ACCESS AND PROTECT CRITICAL SYSTEMS FROM GENERAL IT ENVIRONMENT

Control number	Control title	Control description	Compliance
1.1	SWIFT Environment Protection	**Control Objective:** Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment. **Control Statement:** A segregated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments.	
1.2	Operating System Privileged Account	**Control Objective:** Restrict and control the allocation and usage of administrator-level operating system accounts. **Control Statement:** Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with least privilege access is used. Note: This control is also applicable to the Solution.	
1.3	Virtualisation Platform Protection	**Control Objective:** Secure virtualisation platform and virtual machines (VM's) hosting SWIFT related components to the same level as for physical systems. **Control Statement:** Secure virtualisation platform, virtualised machines, and supporting virtual infrastructure (for example, firewalls) to the same level as physical systems. Note: This control is also applicable to the Solution.	
1.4	Restriction of Internet Access	**Control Objective:** Control/Protect Internet access from operator PCs and systems within the secure zone. **Control Statement:** All general purpose and dedicated operator PCs as well as systems within the secure zone have controlled direct internet access in line with business. Note: This control is also applicable to the Solution.	

CONTROL OBJECTIVE: SECURE YOUR ENVIRONMENT CONTROL PRINCIPLE: REDUCE ATTACK SURFACE AND VULNERABILITIES			
Control number	**Control title**	**Control description**	**Compliance**
2.1	Internal Data Flow Security	**Control Objective:** Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications. **Control Statement**: Confidentiality, integrity, and authentication mechanisms are implemented to protect SWIFT-related application-to-application operator and, when used, jump server-to-application data flows. Note: If an application is spread over several nodes or systems (virtual or physical), then the (application) communication between those nodes also has to be similarly protected.	
2.1.1	Flows to/from the Solution	To complement 2.1 Internal Data Flow Security In scope components: **Data exchange layer:** flows of financial transactions between the local or remote (hosted and/or operated by a third party) SWIFT-related components (interfaces or connectors) and the Solution at application level, they are connected to (directly or through middleware). **Control Statement**: The flows between the Solution and the SIL, AutoClient, or Alliance Gateway Instant need to be protected as per the control 2.1.	
2.2	Security Updates	**Control Objective:** Minimise the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk. **Control Statement**: All hardware and software inside the secure zone and on operator PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied. Note: This control is also applicable to the Solution.	
2.3	System Hardening	**Control Objective:** Reduce the cyberattack surface of SWIFT-related components by performing system hardening. **Control Statement**: Security hardening is conducted and maintained on all in-scope components. Note: This control is also applicable to the Solution.	
2.4	Back-office Data Flow Security	**Control Objective:** Ensure the confidentiality, integrity, and mutual authenticity of data flows between local or remote SWIFT infrastructure components and the back-office first hops they connect to. **Control Statement**: Confidentiality, integrity, and mutual or message-level based authentication mechanisms are implemented to protect data flows between SWIFT infrastructure components and the back-office first hops they connect to. Note: This control is also applicable to the Solution.	
2.5	External Transmission Data Protection	**Control Objective:** Protect the confidentiality of SWIFT-related data transmitted or stored outside of the secure zone as per operational processes. **Control Statement**: Sensitive SWIFT-related data leaving the secure zone as the result of (i) operating system/application back-ups, business transaction data replication for archiving or recovery purposes, or (ii) extraction for off-line processing is protected when stored outside of a secure zone and encrypted while in transit. Note: This control is also applicable to the Solution.	

CONTROL OBJECTIVE: SECURE YOUR ENVIRONMENT CONTROL PRINCIPLE: REDUCE ATTACK SURFACE AND VULNERABILITIES			
Control number	**Control title**	**Control description**	**Compliance**
2.5.1	Customer Data Flow Security	**Control Objective:** Ensure the confidentiality, integrity, and authenticity of data flows between the Solution Provider SWIFT-related applications and their customers. **Control statement**: Communication traffic between the SWIFT customers' site and the Solution Provider's SWIFT infrastructure are protected through secure protocols to support the confidentiality, integrity and mutual authentication of the data flows.	
2.6	Operator Session Confidentiality and Integrity	**Control Objective:** Protect the confidentiality and integrity of interactive operator sessions connecting to the local or the remote (operated by a service provider) SWIFT-related infrastructure or applications. **Control Statement**: The confidentiality and integrity of interactive operator sessions connecting to SWIFT-related applications (local or at the service provider) or into the secure zone is safeguarded. Note: This control is also applicable to the Solution.	
2.7	Vulnerability Scanning	**Control Objective:** Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results. **Control Statement**: Secure zone including dedicated operator PC systems are scanned for vulnerabilities using an up-to-date, reputable scanning tool and results are considered for appropriate resolving actions. Note: This control is also applicable to the Solution.	
2.7.1	Vulnerability Scanning Frequency & Scope	Superseding 2.7 Vulnerability Scanning: Vulnerability scanning must be performed at least quarterly and should include network components (such as routers and switches)	
2.8	Critical Activity Outsourcing	**Control Objective:** Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities. **Control Statement**: Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organisation. Note: This control is also applicable to the Solution.	
2.8.1	Provide Shared Connectivity Services	To complement 2.8 Critical Activity Outsourcing **Control Objective:** Ensure that the Solution Provider provides actual shared connectivity services. **Control Statement**: The Provider must own and operate the SWIFT connectivity components (VPN box and related Alliance Connect Bronze, using two different Internet Service Provider (ISP) or higher used pack, Alliance Lite2 GUI with AutoClient in MultiBic mode, DirectLink and, if used, the SIL, and Alliance Gateway Instant), the compatible Business Applications or Solution, and other customer facing components.	
2.8.2	Outsourcing Critical Activities	To complement 2.8 A Critical Activity Outsourcing **Control Statement**: Critical operations must be performed by the Solution Provider.	
2.8.5	Messaging Monitoring on behalf of customer	To support 2.8 Critical Activity Outsourcing and complement 2.8.3 Critical Activities on behalf of the Customer **Control Objective:** Ensure a consistent and effective approach for the customers' messaging monitoring. **Control Statement**: When the customer outsources the monitoring of its messaging to a Solution Provider, this must be documented in the contractual documentation.	

CONTROL OBJECTIVE: SECURE YOUR ENVIRONMENT CONTROL PRINCIPLE: REDUCE ATTACK SURFACE AND VULNERABILITIES			
Control number	**Control title**	**Control description**	**Compliance**
2.8.7	Limit Access to Customers' Messaging Data	To complement 2.8 Critical Activity Outsourcing **Control Objective:** Protect the confidentiality of the customers' messaging data. **Control Statement**: Unless explicitly requested by its customers, the Solution Provider must not have access to the messages payload on a day to day basis. **Context:** Prevent leakage of customer's messaging data by limiting access to those sensitive data.	
2.8.8	Critical Activities on Behalf of the Customer	To support critical activity performed on behalf of your SWIFT customers and 2.8 Critical Activity Outsourcing **Control Statement**: security-related operations performed by the Solution Provider on behalf of its SWIFT customer using Online Operation Manager (O2M), Secure Channel, the AutoClient, Alliance Gateway Instant, DirectLink or directly Alliance Lite2 or Alliance Cloud must be performed according to strict security procedures agreed between the Solution Provider and the customer. The security-related operations cover (but are not limited to): – PKI certificates administration (such as certificate lifecycle management, RBAC roles assignment) – users management – RMA management – tokens management – access to SIL, Alliance Gateway Instant, DirectLink, AutoClLient folders	
2.10	Application Hardening	**Control Objective:** Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT compatible messaging and communication interfaces and related applications. **Control Statement**: All messaging interface and communication interface products within the secure zone are SWIFT compatible. Application security hardening is conducted and maintained on all in-scope components. Note: For L2BA, this means securing the AutoClient using the Alliance Lite2 Security Guidance.	
2.10.1	SWIFT Compatible Application	To complement 1.1 SWIFT Environment Protection and 2.10 Application Hardening: The Solution Provider must use a SWIFT Compatible Solution (confirmed by relevant labels) for the type of messages they exchange with SWIFT in line with the Alliance Lite2, Alliance Cloud, and Alliance Gateway Instant offering.	

SECURE YOUR ENVIRONMENT PHYSICALLY SECURE THE ENVIRONMENT			
Control number	**Control title**	**Control description**	**Compliance**
3.1	Physical security	**Control Objective:** Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage. **Control Statement**: Physical security controls are in place to protect access to sensitive equipment, hosting sites, and storage. Note: This control is also applicable to the Solution.	

KNOW AND LIMIT ACCESS PREVENT COMPROMISE OF CREDENTIALS			
Control number	**Control title**	**Control description**	**Compliance**
4.1	Password Policy	**Control Objective:** Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy. **Control Statement**: All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed log-in attempts. Similarly, personal tokens and mobile devices enforce passwords or Personal Identification Number (PIN) with appropriate parameters. Note: This control is also applicable to the Solution.	
4.2	Multi-Factor Authentication	**Control Objective:** Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication. **Control Statement**: Multi-factor authentication is used for interactive user access to SWIFT-related applications and operating system accounts. Note: This control is also applicable to the Solution.	

KNOW AND LIMIT ACCESS MANAGE IDENTITIES AND SEGREGATE DUTIES			
Control number	**Control title**	**Control description**	**Compliance**
5.1	Logical Access Control	**Control Objective:** Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts. **Control Statement**: Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties. Note: This control is also applicable to the Solution.	
5.2	Token Management	**Control Objective:** Ensure the proper management, tracking, and use of connected hardware authentication tokens or personal tokens (if tokens are used). **Control Statement**: Connected hardware authentication or personal tokens are managed appropriately during assignment, distribution, revocation, use, and storage. Note: This control is also applicable to the Solution.	
5.3	Personnel Vetting Process	**Control Objective:** Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting in line with applicable local laws and regulations. **Control Statement**: Staff operating the local SWIFT infrastructure are vetted prior to initial employment in that role and periodically thereafter. Note: This control is also applicable to the Solution.	
5.4	Physical and Logical Password Storage	**Control Objective:** Protect, physically and logically, a repository of recorded passwords. **Control Statement**: Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-to-know basis. Note: This control is also applicable to the Solution.	

DETECT&RESPOND DETECT ANOMALOUS ACTIVITY TO SYSTEMS OR TRANSACTION RECORDS			
Control number	**Control title**	**Control description**	**Compliance**
6.1	Malware Protection	**Control Objective:** Ensure that the local SWIFT infrastructure is protected against malware and act upon results. **Control Statement**: Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems and results are considered for appropriate resolving actions. Note: This control is also applicable to the Solution.	
6.2	Software Integrity	**Control Objective:** Ensure the software integrity of the SWIFT-related applications and act upon results. **Control Statement**: A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications and results are considered for appropriate resolving actions.	
6.4	Logging and Monitoring	**Control Objective:** Record security events and detect anomalous actions and operations within the local SWIFT environment. **Control Statement**: Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs. Note: This control is also applicable to the Solution.	
6.4.1	NR Evidences	To complement 6.4 Logging and Monitoring **Control Objective:** Support E2E flow non-repudiation of message/ request emission **Control Statement**: Solution Provider must keep evidences of data submitted/instructions received from its end-customers.	
6.5	Intrusion Detection	**Control Objective:** Detect and prevent anomalous network activity into and within the local SWIFT environment. **Control Statement**: Intrusion detection is implemented to detect unauthorised network access and anomalous activity. Note: This control is also applicable to the Solution.	

DETECT&RESPOND PLAN FOR INCIDENT RESPONSE AND INFORMATION SHARING			
Control number	**Control title**	**Control description**	**Compliance**
7.1	Cyber Incident Response Planning	**Control Objective:** Ensure a consistent and effective approach for the management of cyber incidents. **Control Statement**: The user has a defined and tested cyber incident response plan.	
7.1.1	Customer Security Incident Notification	To complement 7.1 Cyber Incident Response Planning **Control Statement**: The Solution Provider must also notify each impacted SWIFT customer without delay in case of cyber/security incidents compromising the confidentiality, integrity or availability of their data.	
7.2	Security Training and Awareness	**Control Objective:** Ensure that all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities. **Control Statement**: Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access.	
7.3	Penetration Testing	**Control Objective:** Validate the operational security configuration and identify security gaps by performing penetration testing. **Control Statement**: Application, host, and network penetration testing is conducted into and within the secure zone and on operator PCs.	
7.3.1	Yearly Testing	Superseding 7.3 A Penetration Testing: The penetration testing must be performed yearly.	
7.4	Scenario Risk Assessment	**Control Objective:** Evaluate the risk and readiness of the organisation based on plausible cyberattack scenarios. **Control Statement**: Scenario based risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organisation's security programme.	