SWIFT Shared Infrastructure Programme, Security and Operational Framework for 2021

SELF-ATTESTATION

This form should be used to submit your Service Bureau self-attestation of compliance towards the controls of the Shared Infrastructure Programme, Security and Operational Framework for 2021 (SIPSOFv2021).

The SIPSOFv2021 becomes effective on the 1st of January 2021, all service bureaux are expected to be at least partially compliant to all applicable controls, and to be full compliant by the 31st of December 2021.

Service Bureaux may be published as SIPv2021 compliant 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 – SIPSOFV2021

Service Bureau BIC	
I have read the CSCF document	☐
I have read the SIPSOF document	☐
Target date for full compliance against SIPSOFv2021 (DD-MMM-YY)	

Controls in rows with white background are related to the control requirements defined in the Customer Security Controls Framework 2021 (CSCFv2021) from SWIFT Customer Security Program (CSP), for Architecture A1 or A2.
Controls in rows with grey background are related to the control requirements defined in the SIPSOFv2021.

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 SIPSOF (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.	
1.1.3	Network Configuration	To complement 1.1 SWIFT Environment Protection **Control Statement:** The service bureau must ensure that the inbound and outbound connectivity to the service bureau SWIFT infrastructure is restricted to fullest extent possible and maintained.	
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.	
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.	
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.	

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.	
2.2	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.	
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.	
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.	
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.	
2.5.1	Customer Data Flow Security	**Control Objective:** Ensure the confidentiality, integrity, and authenticity of data flows between the service bureau SWIFT-related applications and their customers. **Control Statement:** Communication traffic between the SWIFT customers' site and the service bureau'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.	

CONTROL OBJECTIVE: SECURE YOUR ENVIRONMENT
CONTROL PRINCIPLE: REDUCE ATTACK SURFACE AND VULNERABILITIES

Control number	Control title	Control description	Compliance
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.	
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.	
2.8.1	Provide Shared Connectivity Services	To complement 2.8 Critical Activity Outsourcing **Control Objective:** Ensure that the service bureau provides actual shared connectivity services. **Control Statement:** The service bureau must own and operate the SWIFT connectivity (VPN and SWIFTNet Link, and optionally an Alliance Gateway or alternative gateway solution) and/or the SWIFT messaging interface (Alliance Access, AMH or other compatible messaging interface product).	
2.8.2	Outsourcing Critical Activities	To complement 2.8 A Critical Activity Outsourcing **Control Statement:** Critical operations must be performed by the service bureau.	
2.8.7	Limit Access to Customers' Messaging Data	To complement 2.8 A Critical Activity Outsourcing **Control Objective:** Protect the confidentiality of the customers' messaging data. **Control Statement:** Unless explicitly requested by its customers, the service bureau operator must not have access to the messages payload. 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 A Critical Activity Outsourcing **Control Statement:** Security-related operations performed by the service bureau on behalf of its SWIFT customer must be performed according to strict security procedures agreed between the service bureau 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 managements – RMA management – tokens management	
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.	

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.	

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.	
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.	

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.	
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.	
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.	
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.	

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.	
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.	
6.3	Database Integrity	**Control Objective:** Ensure the integrity of the database records for the SWIFT messaging interface and act upon results. **Control Statement:** A database integrity check is performed at regular intervals on databases that record SWIFT transactions and results are considered for appropriate resolving actions.	
6.4	Logging and Monitoring	**Control Objective:** Ensure the integrity of the database records for the SWIFT messaging interface and act upon results. **Control Statement:** A database integrity check is performed at regular intervals on databases that record SWIFT transactions and results are considered for appropriate resolving actions.	
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.	

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 service bureau 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 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.	

MAINTAIN SWIFT SERVICES AVAILABILITY SET AND MONITOR PERFORMANCE			
Control number	**Control title**	**Control description**	**Compliance**
8.1	Define SLA	**Control Objective:** Ensure availability by formally setting and monitoring the objectives to be achieved. **Control Statement:** SLA and NDA must be part of the contractual agreement and cover critical activities performed on behalf of the SWIFT customers and incidents escalation to them.	
8.4	Capacity Management	**Control Objective:** Ensure availability, capacity, and quality of service to customers. **Control Statement:** the service bureau must demonstrate an effective capacity planning process driving infrastructure changes when required.	
8.5	Early Availability of SWIFTNet Releases and of FIN Standards	**Control Objective:** Ensure early availability of SWIFTNet releases and of the FIN standards for proper testing by the customer before going live. **Control Statement:** The service bureau must implement: – SWIFTNet messaging services software upgrades at least 1 month before products end of life – SWIFT Standards releases at least 6 weeks before the annual FIN standard changeover	

MAINTAIN SWIFT SERVICES AVAILABILITY ENSURE AVAILABILITY THROUGH RESILIENCE			
Control number	**Control title**	**Control description**	**Compliance**
9.1	Local Resilience	**Control Objective:** The service bureau must ensure that the service remains available for customers in the event of a local disturbance or malfunction. **Control Statement:** The service bureau must provide and test formal monitoring and operational measures to allow timely activation of a local fall-back solution at the primary site to be able to cope with the customers' traffic.	
9.2	Site and Systems Resilience	**Control Objective:** The service bureau must ensure that the service remains available for customers in the event of a site disaster. **Control Statement:** The service bureau is required to have a disaster recovery site that enable to meet the committed Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	
9.3	Physical Environmental Controls	**Control Objective:** The service bureau must ensure that the service remains available for customers in the event of a disturbance, a hazard, or an incident. **Control Statement:** the service bureau must implement environmental controls that address risks exposures relevant to the location of its data centres.	

MAINTAIN SWIFT SERVICES AVAILABILITY ENSURE AVAILABILITY THROUGH RESILIENCE			
Control number	**Control title**	**Control description**	**Compliance**
9.4	Connect Solidly to the SWIFT Network	**Control Objective:** Availability and quality of service is ensured through usage of the recommended SWIFT connectivity pack. **Control Statement:** The service bureau must only operate Alliance Connect Gold for its primary/active site(s) and Alliance Connect Silver with dual-VPN solution as the minimum for its disaster recovery site(s). Context: – Internet lines have no performance guarantees or managed resiliency and are potentially more prone to (distributed) denial of service attacks/ cyber-attacks. – SWIFT can monitor both Alliance Connect Gold lines and manages the relationship with the Network Partners. – In the case of a connection or line failure, there is an automatic fallback to the other Alliance Connect Gold leased line, thereby limiting service disruptions & keeping it transparent for the service bureau.	
9.5	Resilient SWIFTNet Instant Connectivity to SWIFT Network	Only applicable to Instant Payments **Control Objective:** Availability and quality of service is ensured through (i) the usage of one of the recommended SWIFT connectivity packs and (ii) the implementation of two separate active sites as per the SWIFTNet Service Description (section 3.5.2). **Control Statement:** TFor SWIFTNet Instant, the Alliance Gateway Instant infrastructure must be composed of at least two active Alliance Gateway Instant instances located in separate sites, each with different Alliance Connectivity pack. Choice can be done between Alliance Connect Gold, Alliance Connect Silver (Dual-VPN) or Alliance Connect Silver (Single VPN). **Context:** – Internet lines have no performance guarantees or managed resiliency and are potentially more prone to (distributed) denial of service attacks (DDOS)/cyber-attacks. – SWIFT monitors the leased lines and manages the relationship with the Network Partners. – SWIFTNet Instant is designed to automatically recover from connection or line failure. In such case, the message flow is automatically redirected to the remaining Alliance Connect packages.	

MAINTAIN SWIFT SERVICES AVAILABILITY BE READY IN CASE OF MAJOR DISASTER			
Control number	**Control title**	**Control description**	**Compliance**
10.1	Business Continuity Plan	**Control Objective:** Business continuity is ensured through documented plan communicated to potentially affected parties (service bureau and customers). **Control Statement:** The service bureau must have a Business Continuity Plan demonstrating the ability of the service bureau to guarantee the service in case of major incidents and to ensure that customers are aware of, and when requested, have access to a business continuity plan and disaster recovery procedures.	

LIMIT CUSTOMER BUSINESS DISRUPTION MONITOR AND ESCALATE OPERATIONAL MALFUNCTIONS			
Control number	**Control title**	**Control description**	**Compliance**
11.1	Events Monitoring	**Control Objective:** Ensure a consistent and effective approach for the event monitoring and escalation. **Control Statement:** Service bureaux must put in place procedures to detect (on a continuous basis), escalate, and fix errors reported in installation and operations log files of software, hardware, and network supporting SWIFT operations. This monitoring and reporting can be considered as the input trigger to the management of incidents expressed above.	
11.2	Escalation Plan	**Control Objective:** Ensure a consistent and effective approach for the management of incidents (Problem Management). **Control Statement:** The service bureau must document and implement an incident escalation plan.	
11.3	Messaging Monitoring on Behalf of Customer	To support critical activity performed by the service bureau on behalf of SWIFT customers **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 service bureau, this must be documented in the contractual documentation.	
11.4	Customer Incident Notification	**Control Statement:** The service bureau must notify each impacted SWIFT customer without delay in case of a major incident.	
11.5	Customer Support Facility	**Control Objective:** Effective support is offered to customers in case they face problems during their business hours. **Control Statement:** Customer helpdesk and technical level 2 support (including at least one service bureau specialist connectivity as described in control 12.1 Maintain Expertise) must be available during working hours of the service bureau customers (which could be through on call coverage outside the service bureau working hours).	

LIMIT CUSTOMER BUSINESS DISRUPTION ENSURE KNOWLEDGE IS AVAILABLE			
Control number	**Control title**	**Control description**	**Compliance**
12.1	Maintain Expertise	**Control Objective:** Ensure quality of service to customers through SWIFT certified employees. **Control Statement:** the service bureau must have at least: – two employees certified for the SWIFT on-boarding skills – two employees certified for the SWIFT technical skills	