**ISAE 3000 Report on Information Security**
2020

An independent examination of the internal control policies, procedures and controls supporting the SWIFTNet and FIN messaging service for the period 1 January 2020 to 31 December 2020.

Confidentiality notice

This report contains proprietary and confidential information about SWIFT and its suppliers. It is intended for the sole use of the recipient named by SWIFT, and must not be further disclosed outside the recipient's own organisation. If persons outside the recipient's organisation need to have access to this publication, they should request their own copy in writing from SWIFT's Internal Audit department by e-mail to AssuranceQuestions.Generic@swift.com with their full name, institution, BIC, position in the institution, complete address and reason for needing this report. This report is provided for information purposes only. Detailed SWIFT service commitments are contained in the relevant SWIFT service documentation.

Waiver

SWIFT accepts no liability to any party in respect of the content of the ISAE 3000 report.
The terminology used in this ISAE 3000 report may deviate from the terminology used for marketing purposes. The ISAE 3000 glossary describes the terms as used in this ISAE 3000 report.

SWIFT is the trading name of S.W.I.F.T. SC.

# Contents

# Contents

# Contents

# Foreword by the CEO

When I wrote the foreword to last year's ISAE 3000 report, we were facing a rapid escalation of the Covid-19 pandemic around the world. Since then we have all adapted to living and working differently: everyone reading this will have been - directly or indirectly - affected by the pandemic; some will have lost loved ones and our thoughts are with you.

In response to the pandemic, SWIFT has put in place strong measures to protect the health and safety of our employees and community, whilst maintaining very robust business and operational continuity plans which have proven effective. Indeed, despite the challenging external environment, continually evolving threats from cyber-crime and increasing geopolitical concerns, traffic growth has remained solid and system availability very high. SWIFT has also delivered on many of our major strategic initiatives such as the agile transformation and we have defined and communicated a new and compelling strategy to 2022 and beyond.

For 2020 we report consistently strong results, with healthy financial and traffic growth despite continuing challenges including continuing COVID-19, cyber-crime and increasing geopolitical concerns. Our operational robustness ensures that SWIFT is more relevant than ever before, even in an increasingly challenging competitive and geopolitical environment.

In this context, I welcome the opportunity to appraise your of some of SWIFT's major 2020 achievements and key initiatives for 2021 in the areas of security, reliability resilience and competitive posture.

## 2020 – A year of solid performance and innovation

In 2020, FIN traffic grew 10.7% compared to 2019 traffic volumes, for a total of 9.5 billion messages. This is higher than the budgeted growth of 6.9% mainly driven by growth in securities traffic. We recorded six FIN peak days during the year – the most recent was 1 December with 44.2 million messages. Traffic patterns were influenced by high securities and treasury markets volatility in the context of Covid.

FileAct average daily traffic growth is at 26.8% and InterAct average daily traffic decreased by -4.5%. The latter is driven by a specific flow shifting from InterAct to FileAct. Excluding this event, InterAct volumes are growing at 8.9% and FileAct at 9.1%.

We concluded 2020 with 99.999% availability achieved on the FIN core global service (SIPN, SWIFTNet and FIN), which is well above the target of 99.990%. Store and Forward and SWIFTNet achieved 100% availability.

gpi created a strong foundation for our new strategy and remains important to our onward progress. In October, we enhanced our gpi for Corporates service, introducing an inbound tracking capability. This allows banks' corporate customers visibility on incoming payments, enhancing their treasury and forecasting activities. In November, we enhanced our Financial Institutions Transfers service, introducing payment confirmations for MT 202. This extension is an important milestone towards efficient liquidity management and reconciliation.

Our Agile Transformation continues apace. We established a programme to manage the overall delivery of the strategy along with a new Agile tribe to develop the transaction management platform. This is designed to enable SWIFT to be (i) the preferred partner for our customers, (ii) ranked as a top employer in the financial industry, and (iii) known for our agility, speed and ability to adjust to a changing environment.

## Customer Security Programme

Despite the continued prevalence of the pandemic with its increase in generic cyber threats (themed phishing attacks and creation of malicious URL domains) and its increase in the attack surface (remote working, use of 'bring your own devices', unsecured home networks), throughout 2020 the number of sophisticated Advanced Persistent Threat (APT) cyberattacks attempted on SWIFT customers that are aimed at institutional payments fraud has dropped to roughly a third of the historical norms. Experts suggest that, given the extensive reliance on the need for local money-mule networks to perform in-person withdrawals to exfiltrate stolen funds, the effects of travel restrictions and local lockdowns may have limited the ability of threat actors and associated Organized Crime Groups (OCGs) to maintain normal levels of in-person fraudulent operations.

Throughout 2020, the Customer Security Programme (CSP) has continued to drive industry-wide collaboration against the cyber threat. The aim of CSP remains the same - reduce the risk of cyberattacks across the institutional financial services ecosystem, 'raise the bar' of cyber security hygiene through the provision of security controls, and minimise the impact of fraudulent transactions.

# Foreword by the CEO

At the end of 2020, over 89% of all SWIFT customers had re-attested their level of compliance against the CSP controls - these institutions represent over 99% of all FIN message traffic carried across the SWIFT network. For attested customers, the overall compliance level reported by customers for each individual mandatory control ranged between 93% and 99%.

In terms of effectiveness of these CSP measures, the vast majority of funds that are 'attempted' are subsequently 'recovered' through recalling messages and / or freezing the nostro or end-beneficiary accounts.

It is unlikely that the threat actors will stop any time soon given the overall size of 'funds attempted', therefore the entire community must remain vigilant against these sophisticated and well-funded threat actors and be prepared for a long journey.

## Outlook for 2021

In 2021, the execution of our bold new strategy to support the payments and securities businesses of financial institutions through instant and frictionless transactions will be a central focus, in addition to operational excellence in our core services. Our deliverables will create immediate benefits for SWIFT customers and, as development of the transaction management platform gains momentum, will build on each other as we apply a ‘gain-as-you-go’ approach.

As in previous years, we are committed to maintaining our track record of high service availability – with a target of 99.99% production service availability. We continue to work towards minimising the number of customer business incidents, as well as aim for zero ‘data confidentiality’ incidents and zero ‘data integrity’ incidents.

We will continue the phased, multi-year migration of applications to the Red Hat Linux platform and invest in the related monitoring and control systems to enhance our capabilities to operate those platforms in different environments.

Our security investment programme focuses on continuously elevating our cyber capabilities and maturing our first line of defence. By maintaining a comprehensive set of cyber resilience capabilities at expected maturity levels and stepping up our risk and control practices, we are focusing our efforts where they will deliver the most impact.

## Providing assurance

Our ISAE 3000 Report on Information Security controls for the SWIFTNet and FIN messaging service, covering the period from 1 January 2020 to 31 December 2020, demonstrates our continued commitment to best-in-class practices for risk identification and management, information security, reliability and resilience, technology planning, and communication with users, and our commitment to transparency on to the extent to which we meet the high standards we set for ourselves in line with our customers’ expectations for a one-of-a kind critical service provider of systemic importance like SWIFT.

As in previous years, this report covers our SWIFTNet and FIN messaging services and contains the key controls that SWIFT has designed and implemented. The report is aligned to the CPMI/IOSCO "Principles for Financial Market Infrastructures" - Annex F "Oversight Expectations applicable to critical service providers" and the control processes are mapped to the key clarifying questions in CPMI-IOSCO’s "Assessment methodology for the oversight expectations applicable to critical service providers" in Appendix B of this report.

Following a competitive tender, SWIFT’s Board of Directors appointed Deloitte to review and examine the adequacy and effectiveness of SWIFT’s controls in accordance with the guidelines in the standard. ISAE 3000 is the International Standard on Assurance Engagements for “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information”, established by the International Auditing and Assurance Standards Board (IAASB). We are pleased to confirm that they have issued an unqualified opinion.

The report continues to provide substantive information on SWIFT controls as implemented in the SWIFTNet and FIN messaging service using the ISAE 3000 standard. ISAE 3000 is the International Standard on Assurance Engagements for “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information”, established by the International Auditing and Assurance Standards Board (IAASB). Appendix C of the report lists additional information provided by Management for exceptions noted and summarises the actions being taken to address them.

# Foreword by the CEO

The SWIFT Executive Committee hope you will find this report useful in helping you assess the security of the SWIFT messaging infrastructure and services. As always, we welcome and encourage all comments, feedback and future dialogue on this report.

22 March 2021

Javier Pérez-Tasso

CEO | SWIFT

# Management Statement

As the Management of the Society For Worldwide Interbank Financial Telecommunication SC ('SWIFT'), we are responsible for the identification of control objectives relating to the provision of SWIFTNet and FIN messaging services and the design, implementation and operation of SWIFT's controls to provide reasonable assurance that the control objectives are achieved.

The service and control related descriptions in sections A to D and sections 1 to 5 has been prepared for the target audience as set out in section C1 of this report who have used the SWIFTNet and FIN messaging services during some or all of the period from 1 January 2020 to 31 December 2020, who have a sufficient understanding of the following:

- The nature of the service provided by SWIFT.
- How SWIFT's system interacts with user entities, subservice organisations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how they interact with related controls at SWIFT to achieve SWIFT's control objectives.
- User entity responsibilities and how they may affect the user entity's ability to effectively use SWIFT's services.
- The risks that may threaten the achievement of SWIFT's control objectives and how controls address those risks.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of SWIFT's controls are suitably designed and operating effectively, along with related controls at SWIFT. The description does not extend to controls of the user entities.

The Management of SWIFT confirms that:

a) The service and controls related descriptions in sections A to D and sections 1 to 5 fairly presents the SWIFTNet and FIN services for processing users' messages during the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the in-scope services were designed and implemented, including:

   – The types of services provided;

   – The procedures, within both automated and manual systems, by which messages were initiated, recorded, processed and transferred to users;

   – How the processes dealt with significant events and conditions;

   – Relevant control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organisation's controls; and

   – Other aspects of our control environment, risk assessment processes, information systems (including the related business processes) and communication, control activities and monitoring controls that were relevant to the processing of user messages.

   (ii) Includes relevant details of changes to the SWIFTNet and FIN messaging services during the period from 1 January 2020 to 31 December 2020; and

   (iii) Does not omit or distort information relevant to the scope of the processes being described, while acknowledging that the description is prepared to meet the common needs of a broad range of users and their auditors and may not,

# Management Statement

therefore, include every aspect of the processes that each individual user may consider important in its own particular environment.

b) The controls related to the control objectives stated in section 1 to 5 were suitably designed and operated effectively during the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that:

   (i) The risks that threatened achievement of the control objectives stated in the description were identified;

   (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

   (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the previously outlined period.

22 March 2021

Javier Pérez-Tasso

CEO | SWIFT

Deloitte Consulting & Advisory SCRL
Gateway Building
Nationale Luchthaven 1J
B-1930 Zaventem

Phone: +32 2 800 20 00
Fax: +32 2 800 20 01
www.deloitte.be



To: The SWIFT Board of Directors

*Scope*

We have been engaged to report on the description provided by the Society for Worldwide Interbank Financial Telecommunications SC ('SWIFT' or "service organisation") of the SWIFTNet and FIN messaging services ('SWIFTNet and FIN' or 'system') in Sections A to D and 1 to 5 of this report throughout the period 1 January 2020 to 31 December 2020 (the 'description'), and on the design and operating effectiveness of controls related to the control objectives stated in the description. The description includes manual and automated controls established by SWIFT to support SWIFTNet and FIN messaging services which comprise of:

- The FIN messaging service, including FIN Copy;
- The SWIFTNet messaging service, including SWIFTNet InterAct, SWIFTNet FileAct, SWIFTNet Copy, SWIFTNet Browse and SWIFTNet WebAccess; and
- The SWIFTNet Link and SWIFTNet Minimal Footprint software.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the SWIFT's controls are suitably designed and operating effectively. We have not evaluated the suitability or operating effectiveness of such complementary user entity controls.

Information about the system included in Appendix A to C is presented by SWIFT to provide additional information to users and is not a part of the SWIFT's description of controls. The information in Appendix A to C has not been subjected to the procedures applied in the examination of the aforementioned description of the system and, accordingly, we express no opinion on the information.

*Service Organisation's Responsibilities*

SWIFT is responsible for: preparing the description and accompanying statement included at section titled "**Management Statement**", including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

*Our Independence and Quality Control*

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

*Security Auditor's Responsibilities*

Our responsibility is to express an opinion on the SWIFT's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements other than Audits or Review of Historical Financial Information," issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the

controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the security auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described in section titled "**Management Statement**".

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

*Limitations of Controls at a Service Organisation*

SWIFT's description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual user may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

*Opinion*

Our opinion has been formed on the basis of historical information and the matters outlined in this report. The criteria we used in forming our opinion are those described in section titled "**Management Statement**". In our opinion, in all material respects:

a. The description fairly presents the SWIFTNet and FIN messaging services system as designed and implemented during the period from 1 January 2020 to 31 December 2020;

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the period 1 January 2020 to 31 December 2020 and users applied the complementary user entity controls contemplated in the design of SWIFT's controls throughout the period 1 January 2020 to 31 December 2020; and

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period 1 January 2020 to 31 December 2020.

*Description of Tests of Controls*

The specific controls tested and the nature, timing and results of those tests are listed in Sections 1 to 5 which should be read along with the informative summary provided in the section "Information provided by the Security Auditor".

*Intended Users and Purpose*

This report, including the description of tests of controls and results thereof in Sections 1 to 5 and the informative summary provided in the section "Information Provided by the Security Auditor", is made solely for the use of SWIFT and solely for the purpose of reporting on the control activities at SWIFT, in accordance with the agreed terms of our engagement. Without affecting for any purpose or on any basis our duties owed solely to SWIFT in connection with this report, we understand that it is intended by SWIFT that this report will be made available for the information of members and user entities of the SWIFTNet and FIN messaging services system of SWIFT during some or all of the period 1 January 2020 to 31 December 2020, practitioners providing services to such user entities and prospective

Deloitte.



user entities and oversight authorities as described in Section C1 of the report who have sufficient knowledge and understanding of the following:

- The nature of the service provided by SWIFT;
- How SWIFT's system interacts with user entities, subservice organisations, and other parties;
- Internal control and its limitations;
- Complementary user entity controls and how they interact with related controls at SWIFT to achieve SWIFT's control objectives;
- User entity responsibilities and how they may affect the user entity's ability to effectively use SWIFT's services; and
- The risks that may threaten the achievement of the Service Organisation's control objectives and how controls address those risks.

We permit the disclosure of this report, in full only, including the description of tests of control activities and results thereof, by SWIFT at its discretion to the parties specified above, to enable those parties to verify that a Security Auditor's report has been commissioned by SWIFT and issued in connection with the control activities of SWIFT, and without assuming or accepting any responsibility or liability to those parties on our part. Our report must not be recited or referred to in whole or in part in any other document not made available, copied or recited to any other party, under any circumstances, without our express written consent. To the fullest extent permitted under law, we do not accept or assume responsibility to anyone other than SWIFT's directors as a body and SWIFT for our work, for this report or for the opinions we have formed.

DocuSigned by:
Bert Truyman
2EA28F1460354D6...

**Deloitte Consulting & Advisory SCRL**

Represented by Bert Truyman

Brussels, Belgium
22 March 2021

# About SWIFT

## 1.1 A1 Introduction

SWIFT is a global member-owned cooperative and provider of a platform for messaging and standards for communicating. SWIFT offers products and services to facilitate access and integration, identification, analysis and regulatory compliance.

SWIFT's messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories.

Whilst SWIFT does not hold funds or manage accounts on behalf of customers, it enables the global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby facilitating global and local financial flows, and supporting trade and commerce all around the world.

## 1.2 A2 Governance structure

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

The SWIFT By-laws define the objective of the company and contain the fundamental rules on the admission of shareholders, shareholding, the election and functioning of the Board of Directors, and holding of General Meeting.

SWIFT has a Board of up to 25 independent directors elected by the Members. The Board is responsible for providing leadership in strategy, deciding on policy matters and exercising proper supervision and control. The Board has delegated the day-to-day management of the company to the Chief Executive Officer (CEO).

Information security and risk management within SWIFT are core functions and responsibility of the CEO and the Executive Committee (ExCo). The CEO is ultimately accountable to the Board for ensuring proper security of SWIFT's operations.

The Board has entrusted three of its committees with particular oversight functions with respect to information security and risk management within SWIFT, under specific terms of reference. These committees are:

- The Audit and Finance Committee (AFC), which is the oversight body for the audit process of SWIFT's operations and related internal controls, commits to apply best practice for audit committees so as to ensure best governance. It exercises oversight in the following areas:
  - Accounting, Financial Reporting and Control;
  - Legal and Regulatory Oversight;
  - Security;
  - Ethics Programs;
  - Budget, Finance and Financial Long Term Planning;
  - Risk Management; and
  - Audit Oversight.
- The Technology and Production Committee (TPC), which provides technical advice and guidance to the SWIFT Board and to SWIFT Executives on the development, implementation and roll out of SWIFT's products and services, including confidentiality, integrity and availability. This committee also reviews SWIFT's operational performance, technology evolutions and risks in its operations and product development.
- The Franchise Risk Committee (FRC), which provides advice and guidance to the Board and to the SWIFT executives regarding SWIFT's key risks, including strategic and operational risks. The FRC works in conjunction with the AFC and TPC.

Two management committees, composed of staff members of SWIFT, assist the Executive Committee in meeting its security responsibilities. These committees are:

- The Security Council (SC), which oversees security-related decisions and impacts; and

- The Security and Reliability Committee (SRC), which helps to ensure consistency in oversight of the definition, implementation, and improvement of the security control framework and acts as a reviewer for the Security Council.

Internal Audit (IA) performs a number of audits which are listed in the quarterly revised priority-based audit plan. A subset of these audits supports the independent Security Auditor's examination of the internal control policies, procedures and controls supporting the SWIFTNet and FIN messaging services.

Chief Risk Officer (CRO) Office provides the mechanisms for the assessments of company risks and facilitates risk assessments relating to relevant operational, strategic, reputational and financial risks per the Enterprise Risk Management (ERM) framework.

Under a special arrangement, the National Bank of Belgium, with the support of the G10[1] central banks, performs the oversight of SWIFT. The issues discussed can include all topics related to systemic risk, confidentiality, integrity and availability. SWIFT is overseen because of its importance to the functioning of the worldwide financial system, as a provider of messaging services.

## A3 Organisational structure

This section describes the organisational structure at SWIFT.

## A3.1 The Executive Committee

The Executive Committee consists of the CEO, the Chief Financial, Corporate, Information, Product, Strategy, Customer Experience and Business Development Officers. The General Counsel and Chief Risk Officer report directly to the CEO. The Chief Auditor reports to the Chair of the Audit and Finance Committee of the Board.

## A3.2 The regions

SWIFT is a customer-centric organisation. The five regions in the Business Development group underpin SWIFT's global organisation:

- Americas and UK
- Europe North
- Europe South
- Middle East & Africa
- Asia Pacific

The regional responsibilities include client relationship management and professional service delivery.

## A3.3 Groups

SWIFT is organised in six groups: Strategy, Customer Experience, Corporate Office, Finance, Product and Technology Platform. They work seamlessly with the Corporate Functions (See A3.4) to deliver SWIFT's strategy.

### A3.3.1 Strategy

Key priorities of this group are:

- Determine the Strategic direction of the company cross payments, securities, compliance and data
- Provide market insights, including competitive landscape

[1] Belgium, Canada, France, Germany, Italy, Japan, The Netherlands, United Kingdom, United States, Switzerland, Sweden and The European Central Bank.

### A3.3.2 Customer Experience

The Customer Experience group brings together all customer delivery teams and supports the end-to-end journey experienced by our customers. This entails includes:

- Customer Services Operations, responsible for the customer on-boarding process including internal KYC, membership changes, the order-to-activation process for central applications and services and related data and customer security management.
- Global Support Delivery, responsible for the delivery of 24/7 customer support, operational status information to customers, service management and proactive support to our most critical customers and MIs, and for maintenance and Care services.
- Knowledge Delivery, responsible for creating, delivering and maintaining all product documentation, service descriptions and SWIFTSmart trainings.
- Standards Development supporting community engagement to define and deploy global and local standards.
- Global Services delivering business and technical assessments; design and integration; onboarding, implementation and adoption services; tailored learning; and project management.
- Customer Security engaging with the community on the Customer Security Program and the evolving cyber threats.
- Campaign and Customer Contact Data Management, responsible for delivering important operational information and guidance to our customers, for instance on mandatory releases, and for conducting customer satisfaction surveys.
- Information Products Data Collection, responsible for collection and maintenance of customer data in SWIFT's shared services reference products (KYC and SWIFTRef portfolios)

### A3.3.3 Corporate Office

SWIFT's Corporate Office consists of three groups. Communications, Human Resources, and the CEO Office:

- SWIFT's Communications group is responsible for the end-to-end communications strategy and execution across the globe, both internal and external;
- Human Resources (HR) group is responsible for all personnel-related policies and for ensuring adherence to associated local laws and regulations; and
- CEO office is responsible for alignment, coordination and support of the various CEO, Executive, and Board level activities.

### A3.3.4 Finance

The Finance group is responsible for core finance processes: general accounting, purchasing, treasury, tax, billing and collection activities as well as financial planning, investment decisions and monitoring performance.

### A3.3.5 Product

The Product group brings together SWIFT IT development and testing. It is responsible for the delivery of the core FIN and SWIFTNet messaging solutions, as well as Interface products, business and enterprise applications. The Product group includes the following departments:

- Digital Transformation Office is established to enable the digital transformation of our business and accelerate value delivery through Agile and DevOps practices. It comprises of the following key functions:
  - Agile Center of Expertise (CoE) includes the coaches that train and support the Tribes on agile methodology and works to improve their agile maturity.

  - DevOps team is the responsible for building and standardizing devops capabilities of the agile delivery teams
  - The Program, Project & Dependency Management group manages key delivery programmes and projects and supports the agile tribes in managing dependencies (road managers)
  - Partner Management and PMF team supports Product Tribes and Business Development teams in building efficient, harmonized and customer centric frameworks to support their Go to Market and Partner strategy initiatives
  - Methodology & Controls team defines and maintains the software delivery life-cycle controls for both agile and our legacy waterfall methodology (ENCOMPASS).
  - Market Infrastructure team manages business applications like MIRS (Market Infrastructure Resiliency Service), CREST, EBA, and EURO1/STEP1 and messaging software supporting MI solutions like AUNPP.

- Innovation & Architecture focuses on innovation, user experience and enterprise architecture. It accelerates and de-risks product development, ensures our solutions meet user needs and assures that our products and systems are technically robust and scalable. It is composed of, among others:
  - The Innovation team, which is responsible for product exploration, ecosystem development and emerging technology exploration to create new products and services that deliver value to customers, in a manner that supports sustainable business models;
  - The User Experience team which is responsible for designing best-in-class user interfaces for our products and services;
  - The Architecture teams, which are responsible for the definition of the overall enterprise and service architectures to help deliver defined technology solutions. These teams are also responsible for the definition of software requirements to enable delivery of software systems in line with business requirements;
  - The Technology Roadmap team, which is responsible for the governance of 3rd party technology selection by facilitating effective and efficient technology decisions.
- Messaging Services is responsible for the delivery of messaging projects, and the design, development and integration of FIN, SWIFTNet (InterAct, FileAct, Instant) and MI solutions such as MI-Channel, T2S and ESMIG.
- The On Premises tribe delivers a number of software products operated by SWIFT clients. The portfolio includes a messaging interface (Alliance Messaging Hub), a long term archiving product (Alliance Warehouse) as well as a number of connectivity products (Alliance Gateway, Alliance Gateway Instant, Payment Gateway and SWIFTNet Link).
- Applications & .Com Services is responsible for the delivery of Alliance Managed Operations (AMO) server, swift.com, sibos.com, CLS-TPS (Continuous Link Settlement – Third Party Service), MyStandards, Standards tools and SWIFT Translator.
- API, Identity & Complementors (APIIC) Tribe is focused on delivery of solutions for APIs, Identity and Access Management (including WebAccess) and Platform Partners. The tribe consists of these 3 clusters with several squads within each cluster, wherein the squads focus on very specific areas within those clusters.
- The Financial Crime Compliance (FCC) Tribe is responsible for the Sanctions and Fraud products and services part of SWIFT Financial Crime Compliance portfolio. FCC manages the end2end delivery of: Sanctions/Transactions Screening, Name Screening, List Management Service, Sanctions Testing Service, Payment Controls Service.
- The Journey to Cloud (J2C) Tribe is focussed on the delivery of the following portfolio: Alliance Lite2, Lifeline, L2BA and ARG - Alliance Access/Entry including IPLA, standalone versions and connectors, Web Platform - Alliance Cloud and SWIFT Integration Layer (SIL).
- The Data & Analytics Tribe is focused on the delivery of Data services to our internal customers, partners and SWIFT community through a variety of channels, by leveraging internal and external data sources and analytics capabilities. Today, the tribe consists of solutions that can be grouped as:

Compliance (KYC – Know Your Customer and FCI - Financial Crime Intelligence), Transaction Data (Watch and Observer), Reference Data Services (SWIFTRef and CRDP – Common Reference Data Platform) and Exploration – discovering future potential.

### A3.3.6 Technology Platform

The Technology Platform group is essential for the day-to-day delivery of the SWIFT services. It manages and operates the services used by customers on a 24/7 basis including the running of SWIFT's operational centres and global network.

Within Technology Platform, each team focus on managing and safeguarding SWIFT's infrastructure and systems, to ensure availability of the messaging services:

- In partnership with internal and external stakeholders, the Command Centre and Business Continuity's mission is to ensure that the SWIFT Ecosystem is trusted and able to deliver under exceptional circumstances through business continuity planning, incident prevention, management, and communications;
- Strategic Operations (SO) drives strategic initiatives and ensures readiness by being involved in programmes and projects from inception to deployment. SO is responsible for operations and support readiness, core operational processes and ISAE 3000 compliance;
- Production Operations (PO) is responsible for the 24/7 delivery of services to our customers, managing the messaging service infrastructure, incident and problem handling and the deployment of software releases. PO is also responsible for facilities management of the operating centres as well as other sites;
- Enterprise Services (ES) manages all non-production infrastructure, systems and services, to include Office Automation and Enterprise systems environments and services as well as internal network services. ES also focuses on the end to end delivery of the internal, some non-core external and development / test services;
- Platform Services is responsible for the design and implementation of the self-service standardised infrastructure and platform technical capabilities on behalf of the product and service delivery teams to ensure the availability and security of existing services; and
- Tooling Services is responsible for the standardisation of tools and analytics capabilities to enable the efficient and innovative delivery of products.
- Global Security has a mission to keep SWIFT and its ecosystem safe. It ensures that teams at SWIFT are aware of the risks and threats, and that security is an integral part of SWIFT products and services. It includes the following teams:
  - Cyber Fusion Centre – to ensure global awareness, detection and response to cyber incidents;
  - Security Engineering manages the operational security capabilities to prevent, detect and react to security threats and attacks targeting SWIFT and the customer's infrastructure connecting to SWIFT, based on internal and external intelligence and in line with the needs of the business;
  - Corporate Security focuses on the protection of people working for SWIFT. Corporate Security advises on the protection of people, information and other critical infrastructure assets through physical security measures;
  - Security for Data, Applications & Services' (SDAS) mission is to support the Software Development Lifecycle (SDLC) in all aspects related to applications and services security, ensuring technical security controls are appropriately defined and implemented for SWIFT applications, products and services;
  - Policy, Compliance & Analytics mission is to manage information security controls and requirements, provide an independent view on compliance to key controls, and enable visibility on key security metrics;
  - The mission of Security Strategy, Risk and Execution (SSRE) is to manage and implement the information security risk management policy and framework, enterprise security architecture, cyber resilience practices as well as to manage the internal security investment programme;

- The Red Team performs intrusion exercises and security validation activities using adversarial hacking techniques against SWIFT systems to confirm strengths or identify weaknesses;
- Human Security instils a people mindset and company culture to stimulate the right vigilance level and behaviours of all people at SWIFT to protect SWIFT key assets and intellectual property from external and internal unintentional or malicious human action; and
- The mission of the Security Success & Evolution department is to help Global Security to be successful by driving organisational clarity, efficiency and collaboration.

### A3.3.7 Business Development

The Business Development group is responsible for working locally and regionally with customers as a trusted partner for secure financial messaging and other products and services. The group bridges the customer community and SWIFT's product teams that design the products and services for our customers.

## A3.4 Corporate functions

The Legal and Compliance Department supports SWIFT's business operations, strategic goals and innovative initiatives in a manner designed to ensure SWIFT's compliance with applicable laws and regulations, safeguards SWIFT's legal rights and assets, and preserves SWIFT's reputation. This is achieved by providing trusted legal and compliance advice and support to the Board, Management, and all SWIFT Departments, with a view towards continuously fostering legally sound business decisions that align with SWIFT's corporate governance principles. The Legal department reports to the General Counsel who is part of the extended Executive Committee.

Internal Audit enhances and protects organisational value by providing risk-based and objective assurance, advice, and insight. Internal Audit performs a number of audits which are listed in the annual risk-based audit plan and approved each year by the Audit and Finance Committee. A subset of these audits supports the independent Security Auditor's examination of the internal control policies, procedures and controls. The Chief Auditor has a dual reporting line with a direct solid functional reporting line to the Chair of the Audit and Finance Committee and also a direct solid administrative reporting line to the CEO. The Chief Auditor is part of the extended Executive Committee.

The Chief Risk Officer is responsible for reporting on SWIFT's risk profile to the Executive Committee, to the Franchise Risk Committee (FRC) and to the Board, helping them act upon their risk governance responsibility. As part of the extended Executive Committee, the CRO facilitates the identification of the severe and emerging risks. The CRO reports to the CEO.

The CRO Office assists the CRO in maintaining the ERM Framework and in ensuring its consistent application across the three lines of defence. The CRO Office deploys tools, processes, methodologies and trainings in support of risk management activities across the company.

## A3.5 COVID-19 Preparation and Management

SWIFT plans for unforeseen events through robust business continuity planning that is practiced and tested regularly. As a result, SWIFT has provided uninterrupted operations throughout the COVID-19 pandemic, whilst maintaining strong focus on health and safety of its staff.

SWIFT closely monitors advice from national and local authorities as well as worldwide health authorities including the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC) and the European Centre for Disease Prevention and Control (ECDC). SWIFT's Pandemic Steering Committee regularly reviews the situation to preserve sustained operational efficiency and effectiveness.

In addition, SWIFT's systems enabled all employees except those in critical roles to work from home; this will remain normal practice as vaccination programmes are rolled out worldwide and locations are gradually reopened. Staff in critical roles continue to work onsite as they have throughout the pandemic period to maintain the robustness of our services and systems.

Across all SWIFT locations, travel is restricted, major in-person events are postponed, and only essential employees are working on-site. However, we continue to actively engage with our community through forums including monthly digital Sibos sessions and webinars.

# About SWIFT

For work arrangements that require on-site presence, we maintain a healthy work environment by following local guidelines and regulations including enhanced cleaning cycles, wearing masks and social distancing.

The description within this report, including the design and operating effectiveness of relevant controls, was not impacted nor altered as a result of COVID-19.

# About SWIFTNet and FIN

## B1 Introduction

This section provides an overview of SWIFT's layered messaging infrastructure and messaging zones based on a distributed processing architecture with full, built-in redundancy to ensure maximum availability.

## B1.1 Layered messaging infrastructure

The SWIFT messaging infrastructure is composed of the following layers:

- The Secure IP Network (SIPN) level provides basic connectivity at the IP level; and
- The SWIFTNet and FIN messaging level provides advanced message processing, including processing of structured, financial messages with message validation capabilities.

FIN is one of SWIFT's core messaging services for exchanging financial messages. FIN enables financial institutions to exchange individual structured financial messages securely and reliably. SWIFTNet is a real-time messaging system that also offers a store-and-forward delivery mode. FIN is a store-and-forward messaging system, both services offer value-added functionality, such as message copy, broadcasts (FIN only), and online retrieval of previously-exchanged messages.

SWIFTNet is SWIFT's Internet protocol-based messaging platform. It includes the Secure IP network (SIPN) and the SWIFTNet messaging layer. In addition to FIN, SWIFTNet supports InterAct, FileAct, WebAccess/Browse and Market Infrastructure (MI) Channel messaging services.

The following drawing illustrates the layered approach:

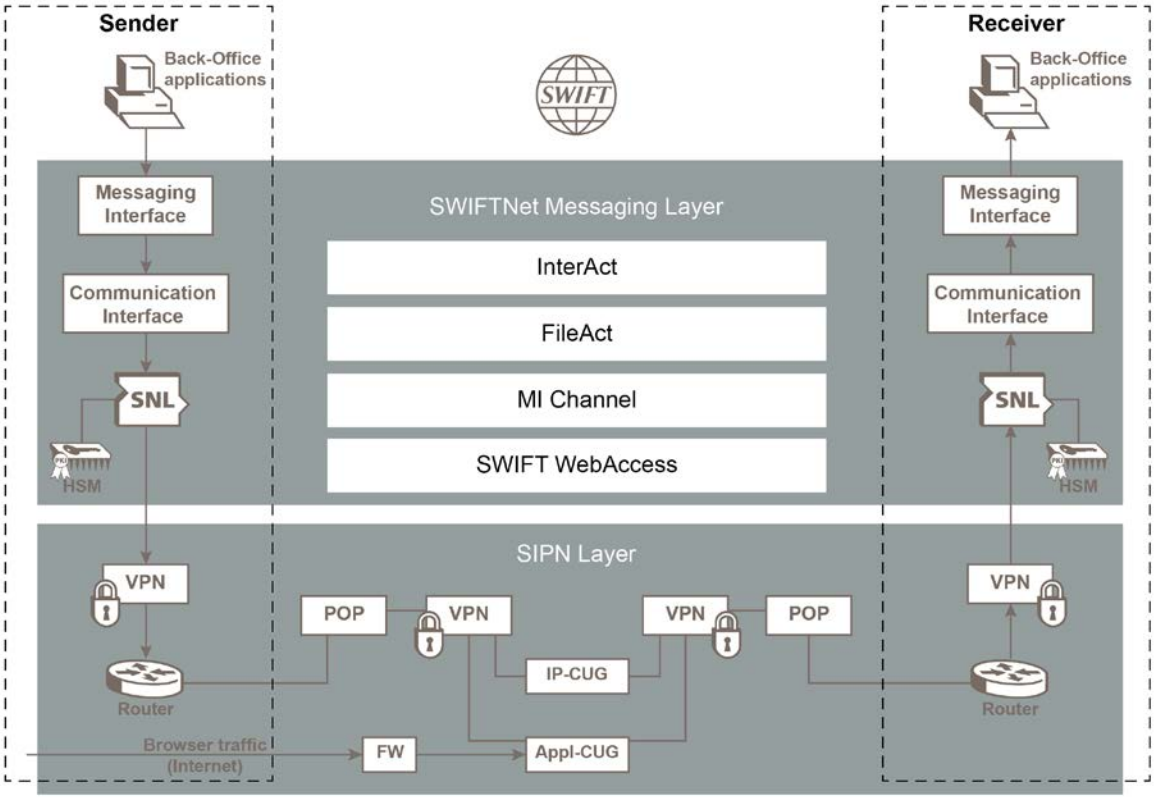


Diagram 1: Layered messaging infrastructure

## B1.2 Secure IP Network layer (SIPN)

The SWIFTNet messaging services run on SWIFT's secure Internet protocol network (SIPN), a protected, private, high availability network.

# About SWIFTNet and FIN

## B1.2.1 Main components and data flows

The Managed Customer Premises Equipment (MCPE) provides the customer with the physical IP-level connectivity to SIPN. It includes a router or a modem and a Virtual Private Network (VPN) box. SWIFT configures and remotely monitors the VPN box, while the customer is responsible for physical security and aspects of its operating environment. In addition, a customer-supplied firewall (FW) separates customers' SWIFTNet interfaces from the MCPE. The firewall must be configured according to SWIFT's rules.

The Points-of-Presence (POP) are facilities provided by SWIFT's Network Partners to connect the customer locally to the SIPN. SWIFT's four Network Partners (AT&T, Colt, Orange Business Services and BT) operate the connectivity between the POP and the VPN concentrator at SWIFT's Backbone Access Points (BAP). Customers contract with these partners to connect to SIPN.

The data flows used for FIN, InterAct, FileAct, WebAccess and MI Channel messaging services (described in the SWIFTNet messaging layer section) leave the SIPN layer and pass through the messaging layer at the SWIFT operating centres (OPCs). This allows SWIFT to provide value added processing described in the SWIFTNet messaging layer section.

The SWIFT Browse flows pass through the Network Closed User Group (IP-CUG) component that verifies whether the two correspondent SNLs are allowed to communicate over Browse. SWIFT WebAccess supports direct access from the Internet. The traffic flows pass through the component labelled Appl-CUG which verifies if a sender is allowed to communicate with a given service provider.

The VPN tunnel between the customers' VPN boxes and SWIFT's VPN concentrators provides data integrity and confidentiality based on the IP-Sec security protocol. The Transport Layer Security (TLS) protocol provides data integrity and confidentiality for SWIFT WebAccess traffic originating from the Internet.

## B1.2.2 SIPN Connectivity

SWIFT provides its customers with three sets of connectivity options providing different levels of throughput and resilience:

- Alliance Connect Bronze is the product for low volume customers. This provides a permanent connectivity to SWIFTNet through one or two Internet connections. Customers can re-use their existing internet infrastructure to connect to SWIFT;
- Alliance Connect Silver and Alliance Connect Silver Plus are the products for medium volume customers, offering connectivity to SWIFTNet through a leased line, managed by a SWIFT Network Partner, combined with an Internet connection. Customers can decide which access method they will use as primary and back-up in function of their traffic pattern; and
- Alliance Connect Gold is the product for high volume customers. It provides connectivity to SWIFTNet through two leased lines managed by one or two SWIFT Network Partners. It offers a traffic segregation feature based on traffic type that allows using both leased lines in parallel.

# About SWIFTNet and FIN

## B1.3 SWIFTNet

### B1.3.1 Main components and data flows

The SWIFTNet messaging layer supports the following messaging services:

- InterAct enables the exchange of messages on a message-per-message basis, and supports the exchange of proprietary formats between correspondents. InterAct offers Store-and-Forward messaging, real-time messaging, and real-time query-and-response options. The InterAct service enables the exchange of MX message types, which are expressed in the flexible XML syntax and developed in accordance with the ISO 20022 standard methodology, many of which have already been published as ISO 20022 standard definitions;
- FileAct enables the transfer of files. It is most efficient when used to transfer large batches of messages, such as bulk payment files, very large reports, or operational data;
- MI Channel (Market Infrastructure Channel) is a messaging channel that is designed to enable customers to access large market infrastructures. It relies on the SWIFTNet Store-and-Forward platform, and optimises the exchange of large amounts of data between the market infrastructure and their participants, while offering a simplified mode of operation and facilitating integration; and
- SWIFT WebAccess/Browse is designed to enable secure, browser-based access from an end user who uses a standard browser, to a service provider's web server over SWIFT. WebAccess/Browse is only for person-to-application use. It is meant for use in the context of HTML-based interfaces. WebAccess/Browse provides strong user authentication to the service provider's application. It also supports the use of non-repudiated transactions (security-sensitive exchanges) when used by the service provider.

SWIFTNet Link (SNL) is SWIFT's mandatory software product for customers of SWIFTNet services. SWIFTNet Link provides the minimum required functionality for technical interoperability between customers that use SWIFTNet services. Its functionality includes transport, formatting, security and service management. It is available under license to vendors and customers for integration with vendor-supplied or customer-developed applications. Functionalities available within the software include transport, formatting, security and service management. The software also provides a number of XML-based Application Programming Interfaces (APIs). SWIFTNet Link enables Alliance Gateway or another third party software to perform application-to-application communication over SWIFTNet services.

Customers can also use Minimal Foot Print (MFP), an alternative to SNL offered to a few Market Infrastructures, whose requirements cannot be addressed by the standard SNL software. In this document, when information related to SNL is mentioned, then the information also applies to this alternative, unless otherwise stated.

SWIFT’s Public Key Infrastructure (PKI) provides a standard security mechanism used at different levels within SWIFTNet. It is embedded in SWIFTNet Link as well as in SWIFT’s internal systems and is used for both user-to-user and user-to-SWIFT security. SWIFT operates the SWIFTNet Registration Authority (for user registration and revocation), the SWIFTNet Certification Authority (for PKI certificate issuance and renewal) and the Certificate Directory (for PKI certificate distribution).

The use of the Hardware Security Module (HSM) is mandatory to support the SWIFTNet PKI services, into the messaging layer. It is a tamper resistant physical device holding PKI secrets used to sign messages. There are two types of HSM that a customer can use:

- Local Area Network (LAN)-based HSM for managing low-to-high traffic volumes or multiple certificates:
  LAN-based HSM boxes are certified to comply with the FIPS 140-2 level-3 security standard and have active tamper detection and response mechanisms that prevent key compromise;
- Universal Serial Bus (USB)-based HSM for managing low traffic volumes and single certificates; and
- USB-based HSMs follow FIPS 140-2 level-2 security standard and offer mechanisms to provide evidence of any attempt at tampering with the system.

The type of HSM a customer uses depends on the hardware platform, traffic volume, and the number of PKI certificates.

### B1.3.2 SWIFTNet messaging features

SWIFTNet offers a number of message validation and storage features:

- The Closed User Group (CUG) feature validates whether correspondents are allowed to communicate over SWIFTNet. The CUG also validates the type of communication. It allows the service providers to define their community of service participants;
- The Message Validation (MVAL) feature is an optional feature for InterAct. It verifies that the contents of a message conform to the applicable message standards;
- Role Based Access Control (RBAC) is an optional feature that validates whether the sender (identified by an Authoriser Distinguished Name) has a role for the service. As an option, it allows the service provider to check the role attributes of the sender for the message or file transmitted;
- The Non-Repudiation Service (NRS) feature is also optional. It time stamps and archives messages and makes them available for later retrieval. A typical reason for retrieval would be when the sender and the receiver have a dispute about the content of the message or the time of exchange;
- For InterAct and FileAct, SWIFTNet Store-and-Forward (SnF) feature allows customers to send InterAct and FileAct messages or files independently from their correspondent's availability. SWIFT delivers them at a time chosen by the receiver. The alternative SWIFTNet delivery mode is real-time and requires the sender and the receiver to be connected at the same time. MI Channel only uses the Store-and-Forward mode; and
- SWIFTNet Copy is an optional function of SWIFTNet, based on Store-and-Forward, which enables senders to copy and distribute messaging data to third parties. SWIFTNet Copy offers two copy modes, Y-Copy and T-Copy. T-Copy routes copies to up to 10 third parties. Y-Copy can be used to solicit authorisation from a third-party. The application service profile of a SWIFTNet service specifies whether use of SWIFTNet Copy is mandatory, optional, or not allowed for a particular request type.

### B1.3.3 Customer interfaces

Messaging interfaces provide application level connectivity to SWIFTNet. They can provide user-to-application and application-to-application types of connectivity. Both SWIFT and its Shared Infrastructure Providers provide SWIFTNet interfaces to SWIFT customers.

SWIFT offers the following software interfaces:

- Communications interface:
  - Alliance Gateway.
- Messaging interfaces:
  - Alliance Access;
  - Alliance Entry; and
  - Alliance Messaging Hub (AMH).

Alliance Web Platform is the Graphical User Interface software for all Alliance products. It exposes functionality of Alliance Gateway, Alliance Access, and Alliance Entry to the end user through a browser.

### B1.3.4 Message flow security

Messaging layer encryption depends on the messaging services used by the customer. InterAct and FileAct data is encrypted at the sender’s SNL and is decrypted at SWIFT by Link Level Encryption (LLE) and/or Transport Layer Security (TLS). After processing at SWIFT, it is encrypted again and is decrypted by the receiver’s SNL. In addition, the sender’s HSM signs each message with its PKI private key. SWIFT verifies the signature to validate the message integrity, and validates the PKI certificate in order to authenticate the sender. The SNL encryption and the PKI validation are standard and cannot be switched off. The sender can also apply a PKI signature for the receiver. The receiver then validates the message integrity and authenticates the sender as well. This end-to-end PKI security is optional. It can be made mandatory at service level if provisioned by the service provider.

# About SWIFTNet and FIN

SWIFT encrypts all messages exchanged through MI Channel while in transit between the customer and SWIFT. This session layer confidentiality is provided by a TLS session, which uses mutual authentication.

SWIFT WebAccess/Browse relies on TLS for encryption and integrity of traffic. SWIFTNet PKI is used to authenticate the end-users.

Direct SWIFT WebAccess access over the Internet (between customer and SWIFT) is secured using TLS and personal tokens and does not use standard SWIFTNet Network layer encryption. It can be made mandatory on a service level if provisioned by the service provider.

## B1.4 FIN application layer

### B1.4.1 Components and flows

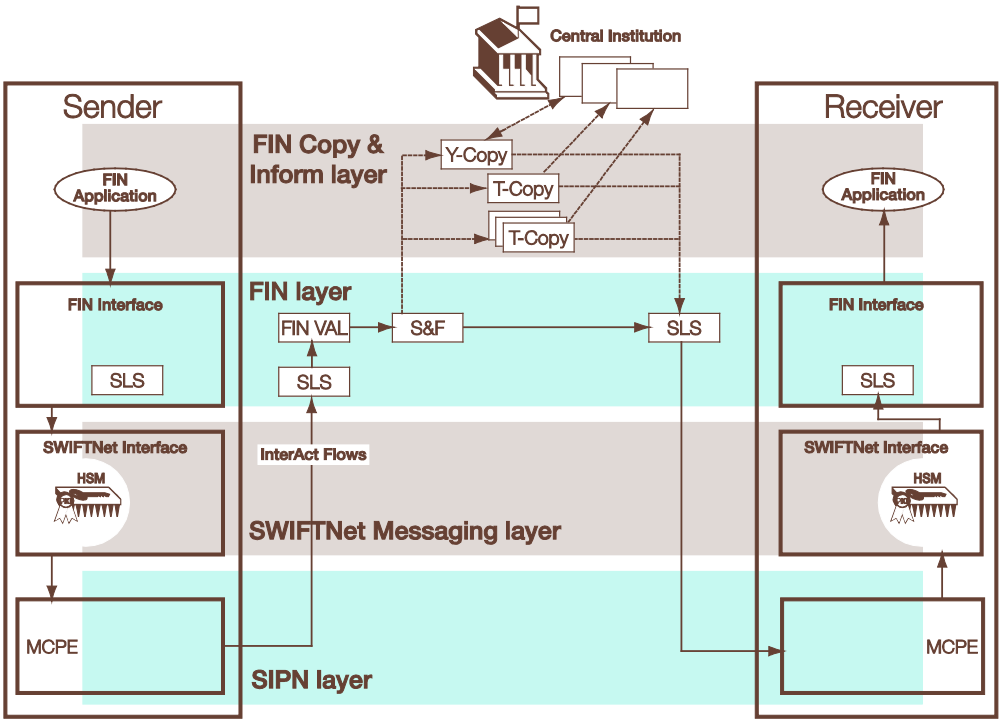


Diagram 2: Main components and data flow of the FIN application layer

FIN is a secure, resilient and structured Store-and-Forward service for financial messages. Value added processing includes:

- Message validation according to SWIFT message standards;
- Delivery prioritisation and monitoring; and
- Message storage and retrieval.

It is based on a distributed processing architecture with full, built-in redundancy to help ensure maximum availability.

FIN uses the InterAct messaging service of SWIFTNet for message exchange. When FIN messages are transported over SWIFTNet, they are wrapped into InterAct messages. When they pass through the FIN layer, the InterAct envelope is removed. FINCopy and FINInform messages are FIN messages that undergo additional processing.

### B1.4.2 FIN system processors

The main components of the FIN application at SWIFT, which are located at SWIFT operating centres, are as follows:

- System Control Processor;

- Slice Processor; and
- Regional Processor

The System Control Processor monitors and controls the entire FIN application. Customer provisioning is performed through the System Control Processor.

The Slice Processor manages the routing and safe storage of messages. Each user destination address (that is, the Bank Identified Code also known as BIC) is defined on a Slice Processor.

The Regional Processors perform input message validation and output message queuing and processing. Each BIC of a financial or a non-financial institution is defined on a Regional Processor.

The FIN Bridge, also located in SWIFT operating centres, connects SWIFT FIN processors and the customer's SWIFTNet connections.

### B1.4.3 FIN messaging features

The FIN application layer includes a number of message validations and storage options features:

- **FIN** validates the message structure against the published FIN message standards. FIN also validates that an entity is subscribed to the proper Message User Group (MUG), when relevant.
- **FIN** stores all sent messages until the receiver retrieves them. If the messages have not been delivered within a fixed timeframe, they are discarded and the sender is notified.
- **Message User Group** (MUG) and **Closed User Group** (CUG) features validate whether two FIN correspondents are allowed to communicate over FIN. They also validate the type of communication and allow the service providers to define their community of service participants. Message User Groups are defined by SWIFT; Closed User Groups are defined by SWIFT-approved service providers.
- **FINCopy** is an optional function of FIN that enables central institutions to receive a copy of and authorise instructions. The FINCopy function is typically used to support market infrastructure services, for example, real-time gross settlement (RTGS) systems, like CHAPS, EURO1, as well as Continuous Linked Settlement (CLS) and Target 2 (T2).
- FINCopy uses the full set of FIN features. In addition, FINCopy offers two copy modes, **Y-Copy** and **T-Copy**. Whereas a normal FIN message is delivered directly to the receiver, the FINCopy service involves a third party, a Central Institution. The Y-Copy mode allows a Central Institution to receive copies of FIN messages, validate the agreed fields of the message, and authorise or prevent message delivery to the receiver. In T-Copy mode, on the other hand, the Central Institution simply receives all or part of the FIN message that has been sent.
- **FINInform** is an optional message copy service for message monitoring. The FINInform service copies all or part of a message to one or more copy destinations using one of two copy modes, Y-copy and T-copy. In T-copy mode the original FIN message is sent to the receiver in parallel with the copy that is sent to the copy destination. The Y-copy mode allows the copy destination to receive copies of FIN messages and authorise or prevent message delivery to the receiver. The FINInform service works on the basis of a Closed User Group and pre-defined service parameters.
- Customers who establish a correspondent relationship and exchange FIN messages over the SWIFT network must first exchange an authorisation to do so using the **Relationship Management Application** (RMA)**.**

### B1.4.4 FIN customer interfaces

The FIN interfaces are capable of generating and processing messages according to the FIN specific standards. FIN interfaces are produced by SWIFT and by other vendors.

### B1.4.5 Message flow security

**Secure Login and Select** (SLS) is a session security mechanism that authenticates the user when the connection to FIN is established until the session is closed. Both the sender and the receiver have to login to FIN, albeit not simultaneously. The integrity and authentication of the login and select message are provided by a PKI signature.

# About SWIFTNet and FIN

If message authentication is required, a customer receives a PKI signature and will use this to verify the integrity of the message and authenticate the sender.

In FINCopy services, an optional PKI signature is calculated on the part of the message that is copied to the Central Institution. This provides authentication and integrity validation for the FINCopy messages that are flowing between the customers (both senders and receivers) and the Central Institution.

## B2 SWIFT messaging zones

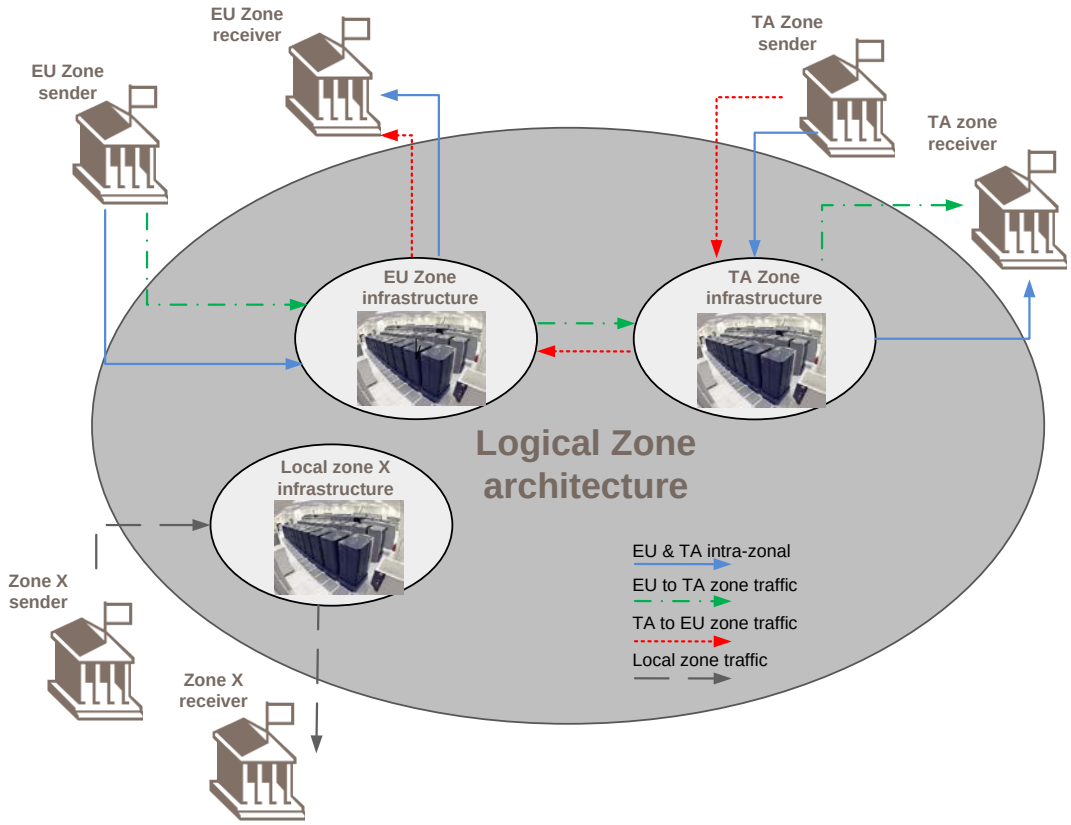


Diagram 3: The SWIFT messaging zonal architecture overview

SWIFT messaging services are capable of operating in multiple zones. SWIFT operates in two zones, namely **European zone** (EU) and **Transatlantic zone** (TA). Any given country is allocated to only one of the global zones for the purpose of SWIFT's messaging services. The messaging services support both intra-zone traffic and inter-zone traffic.

The local zones are segregated from the main SWIFTNet and FIN messaging services. Central Control Centres do not rely on any local zone's infrastructure for the management and monitoring of the SWIFTNet and FIN Services.

In this document, the term "zone" should be interpreted as a global zone unless the term is qualified by the word "local".

# About this report

## C1 Target audience

There are a number of primary parties with an interest in SWIFT providing the SWIFTNet, FIN, FINCopy and FINInform services. These are:

- Members: SWIFT operates the messaging services for the collective benefit of the Members. SWIFT performs the study, development and operation of the means necessary for the transmission and routing of private, confidential and proprietary financial messages;
- The SWIFT Board of Directors: in accordance with the SWIFT By-laws, SWIFT acts in accordance with the directives of the Board, who have the widest powers with respect to acts of disposition or administration;
- Oversight authorities: SWIFT maintains an open and constructive dialogue with oversight authorities on topics of systemic risk, confidentiality, integrity, availability and company strategy; and
- Users of the SWIFTNet and FIN messaging services and their auditors.

For the purposes of this report, the obligations that SWIFT has to the above interested parties, in accordance with the *SWIFT By-laws and Corporate Rules*, in the delivery of messaging services, can be summarised as follows:

- Establishing a proper organisational structure to operate and maintain the SWIFTNet, SWIFTNet Copy, FIN, FINCopy and FINInform messaging services;
- Providing, operating and maintaining the messaging infrastructure for delivery of SWIFTNet, SWIFTNet Copy, FIN, FINCopy and FINInform messaging services while respecting message confidentiality and integrity;
- Co-ordination with the Board and membership on establishing the message standards, membership and participant rules, and management of service and user administration;
- Providing accurate administration of customer configuration and service data; and
- Providing security arrangements, including cyber defence measures, and contingency plans for the messaging services and associated processes and systems.

Notwithstanding this, the report prepared by Deloitte is solely for the use of SWIFT, and they accept no responsibility whatsoever to any other party who might use it.

## C2 Scope of this report

The controls set out within this report are designed to achieve the specific control objectives set forth within this report for the scope specified hereafter, and to mitigate risks which would prevent the achievement of those control objectives. The security audit work of Deloitte is limited to these stated control objectives and controls, and is not intended to assess the other performance obligations that SWIFT has to its primary interested parties, in accordance with performance measures defined to the Board, *SWIFT By-laws*, specific agreements with market infrastructures and other documentation.

### C2.1 CPMI IOSCO requirements for critical vendors

This report contains the controls that SWIFT has designed and implemented to meet the control objectives as defined by SWIFT. This report describes the control processes that SWIFT has implemented as part of its SWIFTNet and FIN service to align with the CPMI/IOSCO "Principles for Financial Market Infrastructures" - Annex F "Oversight Expectations applicable to critical service providers" and the related key clarifying questions in the "Assessment methodology for the oversight expectations applicable to critical service providers". Appendix B contains an explanation and mapping table of the controls against the principles and related clarifying questions.

### C2.2 Messaging and infrastructure components in scope

The scope of this report does not cover SWIFT's products and services in their entirety. As shown in diagram 4, the scope is limited to the following core messaging services and infrastructure components:

- FIN, FINCopy and FINInform;

- InterAct, FileAct, MI Channel and SWIFT WebAccess/Browse;
- Secure IP Network (SIPN); and
- SWIFTNet Link (SNL) software functionality.

Operational processes and equipment required to operate these services are also included:

- Technical components within the SWIFT Operating Centres (OPCs) and Central Control Centres (CCCs);
- Security management processes and related cryptographic processes; and
- Underlying processes (provisioning, operations, support and problem management, deployment, change management).

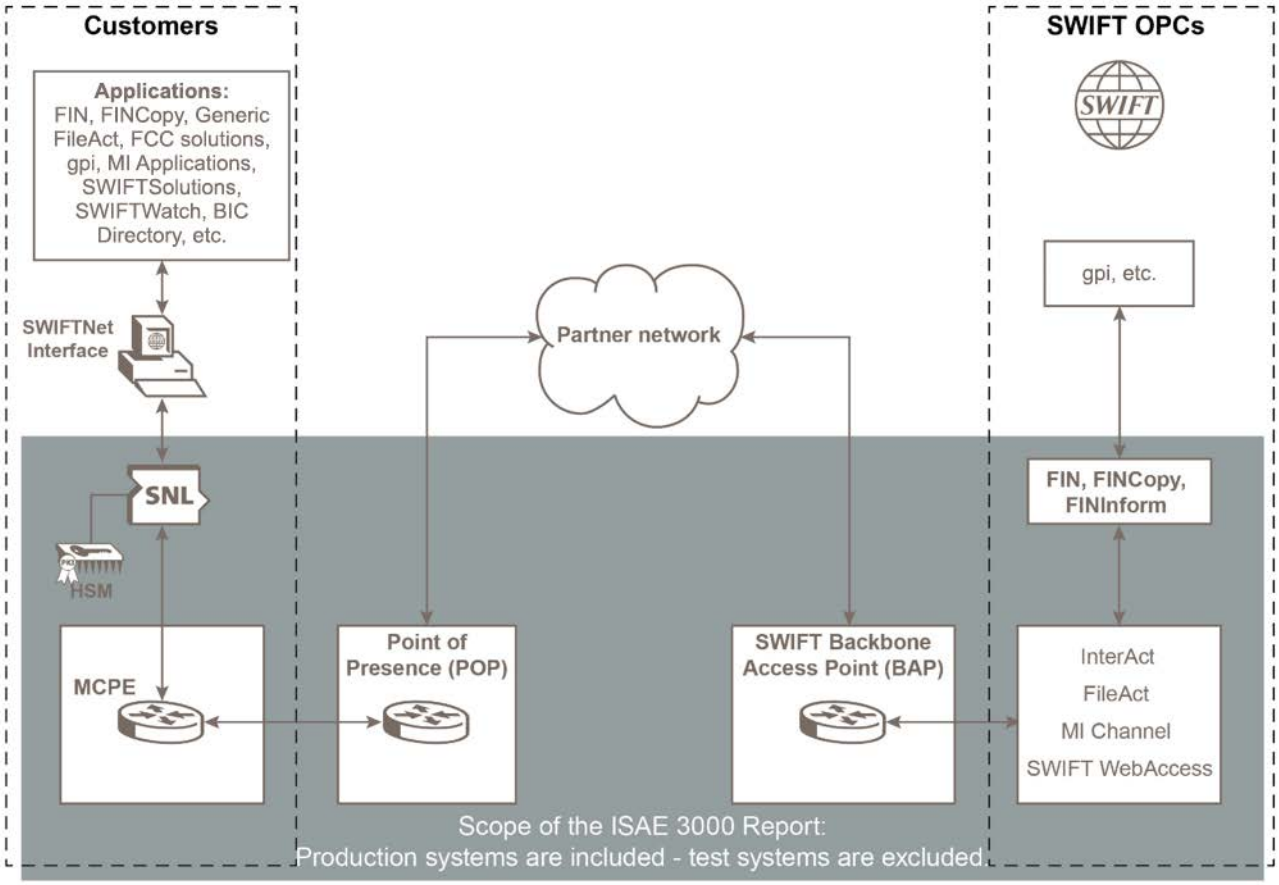


Diagram 4: Messaging and infrastructure components within the scope of this report

This report includes controls over the protection of personal data collected by customers that is contained in message data and processed by SWIFT, to the extent that these controls are exercised by SWIFT in its provision of the SWIFTNet and FIN messaging services and whilst such data are under SWIFT's control.

## C2.3 Areas excluded from the scope

The following areas are not included:

- Specific commitments (if any) beyond the standard commitments found in the SWIFTNet and FIN service descriptions, for example with market infrastructures;
- All aspects which fall under customer responsibility with specific examples described below:
  - Services purchased by customers from Network Partners to connect to SWIFT are not included. However, vendor management, service level agreement (SLA) management and certification with Network Partners (AT&T, Colt, Orange Business Services and BT) are covered;

# About this report

  - While configuration management and operational status monitoring are performed for SWIFTNet Link and customer VPN boxes, customers are responsible for securing their environment with appropriate controls to maintain the confidentiality, integrity and availability of traffic, message and configuration data on its SWIFT systems, and on that segment of its connectivity for which SWIFT is not responsible. The customer-required aspects of security and control of the operating environment are summarised in the User Control Considerations section;
  - Usage of correct sender BIC8 is the customer's responsibility as SWIFT processes message according to the sender BIC8 provided by the customer;
  - Customer connectivity via Alliance Lite or Alliance Lite2 (where SWIFT acts as a service provider), a Service Bureau or another shared infrastructure; and
  - Alliance devices, connectivity with SWIFTNet Link and Relationship Management Application.
- Third-party interfaces, products or services;
- SWIFT.com and SWIFTNet Online Operations manager. However, certain controls over SWIFT.com logical access, change management, configuration management and business continuity supporting order validation, processing and provisioning, online support tools and customer communication are covered. The SWIFT.com services that are explicitly considered in this context are e-Ordering, Online Customer Support (OLCS), Secure Channel, the Download Centre, and the communication of the Operational Status and the Release Timeline;
- The MIRS, 3SKey, KYC and Sanctions services;
- Specific market-focused solutions:
  - CLS Third Party Services;
  - EURO1/STEP1 for EBA Clearing;
  - CREST;
  - SWIFT's Business Intelligence (BI); SWIFT's Applications (Affirmations and Trade Services Utility);
  - SWIFT Standards;
  - SWIFTRef;
  - Customer solutions such as Member-administered Closed User Groups (MA-CUGs) or customer-specific SWIFTNet implementations; and
  - Local zone messaging services.
- SWIFTNet Integration Testbed, FIN Vendor Testbed and Test & Training environments;
- Alliance Lite, Alliance Lite2, Alliance Remote Gateway and the Value Added Network (VAN) Solution for TARGET2 - Securities (T2S);
- Membership and shareholding and BIC registration activities. However, the processes and procedures used to configure, activate, suspend and terminate messaging services are included; and
- Personal data collected by SWIFT (e.g. its own customer contact details) and related controls.

# User control considerations

SWIFT's services are designed with the assumption that certain controls will be implemented by SWIFT users. User organisations, also referred to as customers, should accordingly establish their own internal controls or procedures to complement those of SWIFT.

The following controls should be implemented by user organisations to provide additional assurance that the control objectives described within this report are met. The SWIFT service documentation published on SWIFT.com includes more elaborate explanations of the customer control requirements.

As these items represent only a part of the control considerations that might be pertinent at the user organisations' locations, user organisations' management and auditors should exercise judgment in selecting and reviewing these complementary user controls. The implementation of additional controls may be required to mitigate the user organisations' specific risks.

Furthermore, SWIFT's suggested list of controls is intended to address only those controls surrounding the services and control objectives described in this ISAE 3000 report. Accordingly, this list should not be viewed as a complete list of the controls that users should have in place.

## D1 Customer roles and responsibilities

The security and resilience of the SWIFT's services, and hence the achievement of the full range of control objectives contained within this report, relies in part on certain controls being implemented by customers (as defined in the Glossary).

This Section describes those controls at a high level. It is not intended to be a comprehensive description of all areas of customer's responsibilities, but rather to highlight the main areas of control and to illustrate the reliance placed on customers in ensuring an effective control environment.

As a general principle, the customer is responsible at all times for maintaining the confidentiality, integrity, availability of traffic, message, and configuration data on its SWIFT systems and on that segment of its connectivity for which SWIFT is not responsible under the SWIFT Contractual Documentation. In particular, the customer must ensure that:

- It implements appropriate management principles to ensure (i) only authorised users are created and remain on customer systems; (ii) users are granted physical or logical access to SWIFT services and products on a need-to-know or need-to-have basis only; (iii) all messages or files sent over SWIFT have been duly authorised; (iv) networks, systems, applications are fully segregated based on their criticality; (v) cyber defence controls are implemented;
- It implements appropriate and regularly re-assessed controls to avoid malicious software being exchanged through SWIFT services and products (typically, the scanning of messages sent or received with state-of-the-art and up-to-date virus and malware scanning software), and to avoid that any components or infrastructure used by the customer for the purpose of using SWIFT services and products be used for malicious purposes or cyber-attacks;
- It operates backup procedures and handles backup media according to security practices no less secure than those applied to its production systems and connectivity;
- It installs and uses only that third-party software and equipment that is necessary to access and use SWIFT services and products, and it complies at all times with all proper instructions and recommendations regarding their use (including the timely installation of all critical updates and patches); and
- Compliance with the SWIFT Customer Security Programme (CSP).

The customer must also ensure that its operational environment has been configured for resilience in order to minimise any downtime in the event of a failure of its primary systems or connection. The customer is solely and exclusively responsible to make sure that it develops its own SWIFT service related connectivity contingency and recovery plans.

The customer must also ensure that its SWIFTNet/FIN infrastructure can handle the expected peak traffic for normal conditions and has sufficient capacity to handle urgent traffic.

# User control considerations

## D2 SWIFTNet PKI and Security Officers: specific roles and responsibilities

The customer must maintain two security officers to apply for and manage certificates for the entities within the customer's domain, according to the SWIFT contractual documentation. The customer must also inform SWIFT of registration changes by means of the Secure Channel. For example, offline security officer role granted to new persons, revocation of offline security officer roles of obsolete security officers, and update of address details for secure code card shipping.

The installation and use of the HSM devices are the sole responsibility of the customer. The customer must comply with any guidelines or instructions in force given by SWIFT regarding the use of the equipment.

The customer is expected to comply with the practices for security officers in the Certificate Administration Guide.

## D3 Compliance with SWIFT contractual documentation

The customer must comply with all obligations and other mandatory instructions applicable to it in connection with its use of SWIFT services and products, as set out in the SWIFT contractual documentation or otherwise notified by SWIFT to the customer. There are also particular requirements for customers who are also Service Administrators.

The customer is expected to keep up to date with the amendments of, or supplements to, the SWIFT contractual documentation. The customer must always refer to the latest SWIFT contractual documentation and other service documentation in effect, and must remain aware of the latest available information relating to the SWIFT services and products.

The customer must perform due diligence and apply adequate know-your-customer principles to its counterparts. SWIFT's eligibility criteria and definitions of user categories have not been designed, and must not be relied upon, for these purposes.

Prior to exchanging messages via SWIFT, the customer must seek all necessary or advisable consent and authorisations and enter into all necessary contractual arrangements in order to ensure that no laws, regulations, or third-party rights are violated (including laws and regulations regarding banking, money transmission, securities, money laundering, terrorist financing, economic sanctions, competition, outsourcing and data transmission).

The customer must comply with all relevant laws and regulations regarding the export, re-export, import, and use of any products, software, technology, or materials (including cryptographic technology and materials) comprised in or relating to the provision and the use of SWIFT services and products. The customer is responsible for providing and maintaining current, accurate and complete information and authorised representatives as may be required by SWIFT from time to time in connection with the provision or use of SWIFT services and products.

The customer must inform SWIFT at least three weeks in advance of any change to the customer's infrastructure that can impact the provision by SWIFT to the customer of the SWIFT services and products described in the service description. This includes, but is not limited to, changes to the customer's connection configuration to the secure IP network.

## D4 Compliance with SWIFT services and products and other operating requirements

The customer is responsible for complying with all operating requirements for its use of SWIFT services and products. As applicable, the customer must use a qualified interface and implement the control requirements set out by the SWIFT Customer Security Control Framework, the latest version of which can be obtained on SWIFT.com.

The customer must use only the releases or versions of SWIFT qualified services and products that SWIFT currently supports, as specified in the SWIFT Release Timeline or as otherwise notified by SWIFT.

Consequently, the customer must subscribe to applicable maintenance services and, when using SWIFT software, install all new releases or patches and remove preceding releases or patches, by no later than the date specified in the SWIFT Release Timeline or otherwise notified by SWIFT.

# User control considerations

Customers must, if they appoint a Service Bureau or a Group Hub, consider the impact on their message flow and the allocation of roles and responsibilities between themselves and the Service Bureau or Group Hub. Customers must take due care in the selection and managing of their Service Bureau or Group Hub.

# Information provided by the Security Auditor

This report is intended to provide intended users of SWIFT's SWIFTNet and FIN messaging services as outlined in section C1 of this report with information about SWIFT's controls that may affect the processing of customers' transactions and also to provide customers with information about the operating effectiveness of the controls that were tested. This report is intended to provide such users information about the controls established by SWIFT to achieve the control objectives specified by it in Sections 1 to 5 when combined with an understanding of the following:

- The nature of the service provided by SWIFT;
- How SWIFT's system interacts with user entities, subservice organisations, and other parties;
- Internal control and its limitations;
- Complementary user entity and how they interact with related controls at SWIFT to achieve SWIFT's control objectives;
- User entity responsibilities and how they may affect the user entity's ability to effectively use SWIFT's services; and
- The risks that may threaten the achievement of the Service Organisation's control objectives and how controls address those risks.

Our examination was conducted in accordance with International Standard on Assurance Engagements (ISAE) 3000 Revised, "Assurance Engagements other than Audits or Reviews of Historical Financial Information," issued by the International Auditing and Assurance Standards Board (IAASB). Our testing of SWIFT's controls was restricted to the control objectives and related control activities listed in Section 1 to 5 and was not extended to controls described in the Sections A to D but not included in Section 1 to 5, or to controls that may be in effect at users of SWIFT's services.

It is each user's responsibility to evaluate this information in relation to the controls in place at each user. If certain complementary controls are not in place at the customer, SWIFT's controls may not compensate for such weaknesses.

Our tests of the effectiveness of the controls included such tests as we considered necessary under the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the examination period. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the examination period, for each of the controls listed in this Section, that are designed to achieve the specified control objectives. In selecting particular tests of the operational effectiveness of controls, we considered the following:

- The nature of the items being tested;
- The types of available evidential matter;
- The nature of the testing objectives to be achieved;
- The assessed level of control risk; and
- The expected efficiency and effectiveness of the test.

As part of the examination of SWIFT's controls, Deloitte performed a variety of tests, each of which provided the basis for understanding the framework for controls. These tests determined whether the controls were actually in place and operating effectively with respect to the processing of transactions and the safeguarding of assets in accordance with SWIFT's controls during the examination period. Tests performed to assess operational effectiveness of controls detailed in this Section are described below:

- Inquiry — conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below to corroborate the information derived from inquiry.
- Inspection/scan — Inspected/scanned documents and reports indicating performance of the control activity;
- Observation — Observed the performance of the control multiple times throughout the report period to evidence application of the control activity; and

# Information provided by the Security Auditor

- Reperformance of monitoring activities or manual controls – Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
- Reperformance of control tests performed by SWIFT Internal Audit – Obtained documentation from SWIFT Internal Audit relating to their tests and re-performed the procedures for a judgemental selection of samples examined by SWIFT Internal Audit. Compared any exception items identified with those identified by SWIFT Internal Audit.

### Reporting on results of our tests

The concept of materiality is not applied when reporting the results of our tests of controls for which exceptions have been noted because Deloitte does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently Deloitte reports all deviations.

Our independent procedures to test the design and operating effectiveness of the controls specified by SWIFT as well as the results of those tests are included within Sections 1 to 5 of this report. Although the test procedures and results in Sections 1 to 5 are presented separately, they form an integral part of the information provided by the security auditor.

# 1 Risk identification and management

## 1.1. Introduction

This section describes how SWIFT identifies and manages relevant operational and financial risks and ensures that its risk-management processes are effective.

### 1.1.1. Governance structure

Risk management within SWIFT is a core function and responsibility of the CEO and the Executive Committee (ExCo), who acts under the guidance and supervision of the Board and in particular the FRC.

The Chief Risk Officer (CRO), reporting to the CEO, leads the CRO Office that provides the mechanisms for the assessment of company risks and facilitates risk assessments relating to relevant operational, strategic, reputational and financial risks.

Section A3 describing SWIFT's organisational structure provides an overview of teams specifically involved in risk management.

### 1.1.2. SWIFT Risk management approach

Risk Management within SWIFT is based on an Enterprise Risk Management (ERM) Framework owned by the Chief Risk Officer (CRO).

The objective of the ERM Framework is to ensure that SWIFT has the appropriate tools and practices in place to allow a consistent approach to risk management and reporting, that are also in alignment with the organisation's risk appetite definition. It also aims at promoting risk culture across all areas of the company.

The framework describes the risk governance roles and responsibilities, the risk appetite architecture and the risk management processes. The framework is reviewed on a regular basis and updated when required.

The ERM process at SWIFT is dynamic and continuous, ensuring that risks are adequately identified, analysed, evaluated against the risk appetite, treated (where required), monitored and reported. This approach is aligned with the risk guidance as defined by the International Standard ISO 31000:2018.

The scope of the ERM framework encompasses SWIFT activities whether external, customer facing or entirely internal.

The scope of the framework covers supporting assets (people, network, hardware, software and facilities) and practices required to build, maintain and operate SWIFT activities. It provides a common approach and language for assessing risks and prioritising mitigation actions, enabling the holistic communication and management of risks across SWIFT.

### 1.1.3. Third Party Security Risk management approach

SWIFT has a third party security risk management practice in order to assess and manage cyber risks linked to suppliers who have either direct or indirect access to the information and information systems of SWIFT, or will provide elements (software, hardware, processes or human resources) that are involved in SWIFT products and services. This is managed by SWIFT's Third Party Security Risk Management (3PSRM).

This covers security risks related to:

- Third Party Information Service Providers (3PSP) who provide services not operated by SWIFT; and
- Third Party Technology Vendors (3PTV) who provide specific technology used by SWIFT.

In addition, the Technology Vendor Advisory Council (TVAC) reviews ensure that technology risks are taken into consideration when new technologies are introduced or current technologies are used in new ways.

Vendor managers monitor product and support quality, product lifecycles and evolution. They also work with vendors, as needed, to assist Finance in conducting annual Vendor Financial Due diligence reviews. The information gathered is used to assess vendor and product related risks and plan mitigations as necessary. Significant risk assessments and mitigation actions are communicated to the board TPC as part of the annual Technology Risk Management update.

# 1 Risk identification and management

## 1.2. Control objectives

The following control objectives govern a series of controls applicable to risk identification and management for the SWIFTNet and FIN services:

1. A governance structure is in place to identify and manage risks and monitor the effectiveness of risk management processes; and
2. Risks related to critical suppliers are documented and managed

The sections hereafter describe the different controls in place to meet each of these objectives.

### 1.2.1. Governance structure

Control objective: A governance structure is in place to identify and manage risks and monitor the effectiveness of risk management processes.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | The Board's Audit and Finance Committee's (AFC) mission, scope and composition are described in the AFC Charter, which is reviewed annually and approved by the Board. The AFC meets at least four times per year. The Chair of the AFC debriefs the full Board on the Committee's activities at every Board meeting. Meeting minutes are prepared by the Chief Auditor and after review and approval shared with all Board members.<br><br>The Committee's areas of responsibility include oversight over the Internal Audit function, the security and financial audit mandates, the independence of the Internal Audit function and External Audit firms, accounting, financial reporting and control, budget, finance and financial long term planning. Annually, the Committee reviews the fulfilment of its responsibilities based on an analysis by the Chief Auditor. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the AFC Charter to confirm that it covered the areas of responsibility, mission, scope and composition of the Board's Audit and Finance Committee, and that it was reviewed and approved in the year.<br><br>Inspected the minutes of AFC meetings to confirm that;<br>• minutes were approved and shared with all board members; and<br>• the Committee reviewed the fulfilment of its responsibilities based on an analysis by the Chief Auditor.<br><br>**No relevant exceptions noted** |
| **2.** | The Technology and Production Committee (TPC) provides technical advice and guidance to the Board and to the SWIFT executives on the planning, design, development, implementation, rollout, and maintenance of SWIFT products and services. The TPC also reviews SWIFT's operational performance, and technology and security risks related to its products and services.<br><br>Specifically, the TPC provides:<br>• Guidance in the commercial implementation strategy for the product portfolio.<br>• Guidance in the underlying technology and operational strategy and investments that support the commercial implementation strategy. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of meeting minutes of the Technology and Production Committee (TPC) to confirm that it provided technical advice and guidance to the Board and to the SWIFT executives on:<br>• the commercial implementation strategy for the product portfolio;<br>• the underlying technology and operational strategy and investments that support the commercial implementation strategy;<br>• review on key project progress and operational results; |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | • Guidance and review on key project progress and operational results.<br>• Guidance on IT security and technology risk assessments and mitigation strategies. This includes the areas of systemic risk, operational risk, vendor technology risk, physical security risk and logical security risk (including cyber risk).<br><br>Updates of the information security risk posture are reviewed by the TPC annually. The TPC meets multiple times a year. After each meeting, minutes are produced. | • IT security and technology risk assessments and mitigation strategies. This includes the areas of systemic risk, operational risk, vendor technology risk, physical security risk and logical security risk (including cyber risk).<br><br>Inspected the annual information security report to confirm that the information security risk posture was reviewed by the TPC.<br><br>**No relevant exceptions noted** |
| **3.** | The day-to-day management of the company has been formally delegated by the Board to the CEO, including responsibility for the implementation of policies and procedures in order to ensure that the control and security objectives are achieved. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described<br>• Inspect SWIFT's Board Handbook to confirm that the responsibilities of the CEO, which included the day-to-day management of the company, was documented and approved.<br>• Inspect SWIFT's Information Security Charter to confirm that the CEO governed the implementation of controls, policies and procedures through his position as chairperson of the Executive Committee.<br><br>**No relevant exceptions noted** |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **4.** | The Security and Reliability Committee (SRC) is a management committee that is the primary management body for the CIO, CPO and Chief Security Officer (CSO) for oversight over the definition, implementation and improvement of the Information Security Control Framework.<br><br>It defines and reviews the security strategy. It reviews and approves major policies prior to submission to the Security Council. The SRC performs oversight of major risk analyses, the operational business continuity planning strategy and implementation, cyber defence and intrusion testing strategy and tests, as well as technology and operations-specific control improvement initiatives.<br><br>The SRC meets at least four times a year. After each meeting, minutes are produced. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described<br><br>• Inspect SRC terms of reference to confirm that SRC was the primary management body for the CIO, CPO and Chief Security Officer for oversight over the definition, implementation and improvement of the information Security Control Framework.<br><br>• Inspect a sample of SRC meeting minutes to confirm that SRC:<br><br>– defined and reviewed the security strategy;<br><br>– reviewed and approved major policies prior to submissions to the Security Council; and<br><br>– performed oversight of major risk analyses, the operational business continuity planning strategy and implementation, cyber defence and intrusion testing strategy and tests, as well as technology and operations-specific control improvement initiatives.<br><br>**No relevant exceptions noted** |
| **5.** | SWIFT's Internal Audit department (IA) is led by the Chief Auditor who has a direct solid functional reporting line to the Chair of the AFC and a direct solid administrative reporting line to the CEO. Based on a quarterly reviewed, priority-based audit plan presented to the AFC as part of the quarterly Chief Auditor's report, Internal Audit executes a number of audits, the majority of which have an IT security focus. The plan takes into account strategic initiatives or major projects, risks, contractual assurance obligations and rotational coverage of the audit universe.<br><br>There is a formal process for the reporting and follow-up of resulting audit recommendations, including identification of responsible owners, agreed remedial actions and target dates for recommendation closures. Internal Audit reports are shared with the AFC and a subset of these reports are shared with SWIFT's overseers. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the AFC Charter to confirm that it defined the areas of responsibility, mission and scope of the Chief Auditor.<br><br>Inspected the quarterly reviewed, priority-based audit plan to confirm that this plan was presented to the AFC as part of the quarterly Chief Auditor's report, and took into account strategic initiatives or major projects, risks, contractual assurance obligations and rotational coverage of the audit universe.<br><br>Inspected a sample of audit missions to confirm that the results were shared with the AFC, and that audit recommendations were tracked and followed up for closure.<br><br>**No relevant exceptions noted** |

# 1 Risk identification and management

## 1.2.1 Governance structure (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **6.** | SWIFT conducts background pre-employment and pre-assignment screening, which is subject to local laws and regulations, and is applicable to all new SWIFT employees and temporary SWIFT personnel with access to SWIFT locations and/or systems. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the global screening policy to confirm that the procedures were in line with the control description.<br>• Inspect for a sample of new SWIFT employees and temporary SWIFT personnel, the supporting documentation to confirm that the pre-employment and pre-assignment screening procedures were performed.<br>**No relevant exceptions noted** |
| **7.** | SWIFT conducts background in-employment and in-assignment rescreening, which is subject to local laws and regulations, and is applicable to all SWIFT employees and temporary SWIFT personnel with access to SWIFT locations and/or systems. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the global screening policy to confirm that the procedures were in line with the control description.<br>• Inspect for a sample SWIFT employees and temporary SWIFT personnel with access to SWIFT locations and/or systems, the supporting documentation to confirm that the in-employment and in-assignment rescreening procedures were performed.<br>**Exceptions noted**<br>• For 21 out of 43 temporary personnel, in-assignment rescreening was not performed within the time limits specified by SWIFT processes.<br>• For 8 out of 40 SWIFT employees, in-employment rescreening was not performed within the time limits specified by SWIFT processes. |
| **8.** | The Chief Risk Officer (CRO) owns the Enterprise Risk Management framework. The framework describes the risk governance roles and responsibilities, the risk appetite architecture and the risk management process. The framework is reviewed on a regular basis and updated when required. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Enterprise Risk Management Framework to confirm that: |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | The CRO ensures that risk assessments are performed and that the identified risks are tracked and reported according to the rules defined in the Enterprise Risk Management framework. | – it described the risk governance roles and responsibilities, the risk appetite architecture and the risk management process;<br>– it is owned by the Chief Risk Officer (CRO); and<br>– it was reviewed on a regular basis and updated when required.<br>• Inspect a sample of risk assessments to confirm that identified risks were tracked and reported according to the rules defined in the Enterprise Risk Management framework.<br>Reperformed, for a sample of risk assessments, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **9.** | SWIFT's Franchise Risk Committee assists the Board in its oversight of the Company's management of key risks. It focuses on those areas of risk management that are defined in the Terms of Reference. The Risk Committee works in conjunction with the AFC and TPC. It meets regularly and minutes are produced after each meeting. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Terms of Reference and the SWIFT Board Handbook to confirm that the defined Terms of Reference covered areas of risk management, the roles of the SWIFT's Franchise Risk Committee and its functioning in conjunction with the AFC and TPC.<br>• Inspect a sample of meeting minutes of the SWIFT's Franchise Risk Committee to confirm that the Franchise Risk Committee met regularly and assisted the Board in its oversight of the Company's management of key risks.<br>Reperformed, for a sample of meeting minutes of the SWIFT's Franchise Risk Committee, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, for the Terms of Reference and the SWIFT Board Handbook, SWIFT IA's tests over the documents examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |

# 1 Risk identification and management

## 1.2.1 Governance structure (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **10.** | The Legal department monitors legal and regulatory developments on specific relevant topics in the major jurisdictions where SWIFT operates using various sources (incl. external law firms). The Legal department maintains a registry to track relevant laws and regulations.<br><br>In addition, the legal department monitors the obligations in relation to legal and regulatory requirements pertaining to SWIFT's corporate organisation and conduct. At least every three years, the legal obligations are validated with the external legal counsels in the territories where SWIFT has subsidiaries, by using notably questionnaires, to ensure that the compliance requirements identified remain valid and accurate. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the legislative monitoring procedure to confirm that it required the legal department to monitor legal and regulatory development in the major jurisdictions where SWIFT operates, as well as to monitor the obligations in relation to legal and regulatory requirements pertaining to SWIFT's corporate organisation and conduct.<br><br>• Inspect a sample of updates provided by the external legal counsel to confirm that the legal department monitored legal and regulatory developments on specific relevant topics in the major jurisdictions where SWIFT operated.<br><br>• Inspect a sample of questionnaires sent to SWIFT's external legal counsel and confirm that the legal department monitored the obligations in relation to legal and regulatory requirements pertaining to SWIFT's corporate organisation and conduct.<br><br>Reperformed, for a sample of updates provided by the external legal counsel and a sample of questionnaires sent to SWIFT's external legal counsel, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the legislative monitoring procedure, SWIFT IA's tests over the procedure examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |

# 1 Risk identification and management

## 1.2.2. Supplier risk management

Control objective: Risks related to critical suppliers are documented and managed

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Contracts between SWIFT and its suppliers mandate physical and logical security requirements and liabilities in case of breach. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of supplier contracts to confirm that physical and logical security requirements and liabilities in case of breach were specified.<br>Reperformed, for a sample of contracts, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **2.** | Service level agreements in place with Network Partners and hardware suppliers for the messaging service infrastructure (that is HP Enterprise, Cisco, Juniper) contain:<br>• Agreed performance indicators; and<br>• Reporting and review processes.<br>The SLA reports are reviewed, at documented frequencies, at least once a year and actions are tracked. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the service agreements for a sample of Network partners and hardware suppliers to confirm that service level agreements were in place including agreed performance indicators and reporting and review process.<br>• Inspect a sample of SLAs to confirm that SLA reports were reviewed at documented frequencies, at least once a year, and defined actions were tracked.<br>**No relevant exceptions noted** |
| **3.** | SWIFT has set up the Technology Vendor Advisory Council (TVAC) to assist senior management in technology-related governance for the enterprise. The TVAC serves as an enterprise-wide body to oversee technology decisions.<br>The TVAC reviews and approves specific technology selections as well as specific contracts and amendments, based on business needs.<br>The SWIFT Technology Risk Management framework outlines the objectives and scope of | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the TVAC Terms of Reference to confirm that TVAC was set up to assist senior management in technology-related governance for the enterprise.<br>• Inspect a sample of purchases with technology vendors to confirm that these |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | technology risk management and describes the roles and responsibilities. | were reviewed and approved by the TVAC.<br>• Inspect the Technology Risk Management framework to confirm that it outlined the objectives and scope of technology risk management and described the roles and responsibilities.<br>Reperformed, for a sample of purchases with technology vendors, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, for the TVAC Terms of Reference and Technology Risk Management framework, SWIFT IA's tests over the Terms of Reference and framework examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **4.** | Each SIPN Network Partner must maintain certification as a preferred network provider. To support re-certification, SWIFT assesses on a semi-annual basis:<br>• Service description and geographical coverage;<br>• Backbone SLA commitments;<br>• Operational capabilities in respect of IP virtual private networks;<br>• Pricing; and<br>• Financial health. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of SIPN Network Partners to confirm that they maintained their certification as preferred network provider, and that SWIFT assessed on a semi-annual basis:<br>– Service description and geographical coverage;<br>– Backbone SLA commitments;<br>– Operational capabilities in respect of IP virtual private networks;<br>– Pricing; and<br>– Financial health.<br>**No relevant exceptions noted** |
| **5.** | Once a year, or whenever a new IT vendor is considered, Financial Planning and Analysis performs a financial due diligence on the vendors that are considered strategic, as defined in TVAC TOR, for SWIFT. The results of the analysis together with any potential risks involved with the vendor are provided as input to the Technology Vendor Advisory Council (TVAC) and handled | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | according to SWIFT's Technology Risk Management process. | • Inspect a sample of strategic vendors defined in the TVAC TOR, to confirm that:<br>– a financial due diligence was performed in 2020; and<br>– the output of the financial due diligence and potential risks involved with the vendor were shared with the TVAC and handled according to SWIFT's Technology Risk Management process.<br>Reperformed, for a sample of strategic vendors, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **6.** | SWIFT monitors the service levels, financial health and the security-relevant third party assurance reports of the case management service supplier as defined in SWIFT's Third-Party Risk Management process. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of reports for the case management service supplier to confirm that monitoring of service levels, financial health and relevant third party assurance reports was performed as defined in SWIFT's Third Party Risk Management process.<br>Reperformed, for a sample of reports, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **7.** | SWIFT has established the third party security risk management (3PSRM) process to manage security risks related to its suppliers. As part of this process SWIFT:<br>• Maintains a list of suppliers on which it relies to deliver and support its services;<br>• Gathers relevant information to assess any security risks resulting from the supplier; and<br>• Records and tracks identified security risks for mitigation. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT Third Party Security Risk Management (3PSRM) process description to confirm that the process<br>– was defined to manage security risks related to SWIFT's suppliers; |

| Control Applied | Work Performed / Observations |
|---|---|
| | – maintained a list of suppliers on which SWIFT relies to deliver and support its services; and<br>– gathered relevant information to assess any security risk resulting from the supplier.<br><br>Inspect a sample of third party security risk assessments to confirm that identified security risks were recorded and tracked for mitigation.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.1. Introduction

This section describes how SWIFT implements and maintains appropriate policies and procedures, and devotes sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil commitments to the users of our messaging services.

### 2.1.1. Governance

Information security within SWIFT is a core function and responsibility of the CEO and the Executive Committee (ExCo), who acts under the guidance and supervision of the Board.

Two management committees, composed of staff members of SWIFT, assist the Executive Committee, in meeting its security and risk management responsibilities. These committees are:

- The Security Council (SC), which oversees security-related decisions and impacts; and
- The Security and Reliability Committee (SRC), which helps to ensure consistency in oversight of the definition, implementation, and improvement of the security control framework and acts as a reviewer for the Security Council.

Section A3 describing SWIFT's organisational structure provides an overview of teams among others involved in information security, including Global Security in the Technology Platform group.

### 2.1.2. Security policies and procedures

The SWIFT Corporate Information Security Policy (SCISP) and associated security policies are the central components of SWIFT's Information Security Control Framework. Detailed procedures, security baselines and practical guidelines are in place to support these documents and establish the internal control system.

SWIFT's Data Retrieval Policy, clarifying under which circumstances SWIFT traffic and message data can be retrieved, and SWIFT's Personal Data Protection Policy, setting out the roles and responsibilities of SWIFT, the SWIFT community, and its customers with regard to the processing of personal data, are covered under the personal data protection control objective.

The Executive Committee, Management and staff are responsible for complying with the security policies and baselines. The CEO is ultimately accountable to the Board for ensuring such compliance.

SWIFT has implemented a number of initiatives that enhance security, including a company-wide commitment to adopt many of the principles of ISO 27002, which is the code of practice for information security management. This internationally recognised standard provides wide-ranging security guidelines.

### 2.1.3. Public Key Infrastructure (PKI)

SWIFT uses Public Key Infrastructure (PKI) functionality based on asymmetric cryptography to provide the security features to protect customer messages. Please note the distinction between the Secure IP Network (SIPN) PKI and the SWIFTNet PKI (see also section B1.1).

SWIFTNet PKI operates at the transport and application layers of the SWIFTNet architecture. The PKI is based on two separate key pairs, one used for signing and one for encryption. SWIFT offers PKI features to issue the digital certificates that are used by customers in the end-to-end communication facilities of SWIFTNet. A digital certificate is an electronic file signed by the Certification Authority (CA) that contains the end user's public key and that identifies the owner. The owner of the certificate retains the corresponding private key.

SIPN PKI provides services to the IP layer of the SWIFTNet architecture. The certificates are used upon connection to authenticate the two VPN endpoints and negotiate a symmetric key. This key is then used to encrypt all data exchanged between the VPN box and the VPN concentrator.

### 2.1.4. System access

Systems are categorised into two groups: production and internal systems. Production systems include main message flow systems and production support systems (mainly for monitoring). All other systems, including those used for provisioning, are considered as internal systems.

Personnel access to SWIFT's production systems is implemented on a need-to-have basis as approved by the system owner. The groups responsible for the approval of the access requests and the security

administration of these requests are segregated. The use of defined roles and profiles restricts access to specific functions and prevents inappropriate access.

### 2.1.5. Network access

Networks that carry traffic for SWIFT messaging services are logically separated from networks that are used for internal purposes or local zones. When there is a requirement to link an internal network or local zone infrastructures to a production network, strict security requirements are imposed.

SWIFT has implemented protection mechanisms to restrict and protect access to the SWIFT network. For the SIPN, the MCPE is an integral part of the network. Route filters on the VPN boxes are applied at the MCPE and at the Backbone Access Point (BAP) level to control the flow of data.

For the FIN service, the user's interface to SWIFT allows communication with the FIN messaging service. The FIN interface connects to SWIFT through SWIFTNet using the same access as with other SWIFTNet services.

### 2.1.6. Physical access

The SWIFT operating centres (OPCs) are designed to house mission-critical computer operations. Physical security controls are in place to deter, detect and delay penetration. The following physical security mechanisms have been defined:

- The perimeters around the OPCs are enclosed, guarded and monitored;
- Access tokens and associated Personal Identification Numbers or Biometrics exist for doors and provide audit trails of access to computer floors; and
- Security zones are colour-coded reflecting the different access control mechanisms.

The SWIFT Central Control Centres (CCCs) have similar physical security controls in place as the OPCs to deter, detect and delay penetration. If a CCC is not hosted in an OPC and the control is not operated by SWIFT directly, but indirectly through subcontractors, the physical security policy still applies and monitoring controls are in place.

### 2.1.7. Activation and deactivation of users

Once a new user has registered for a messaging service, SWIFT has defined processes and procedures for their activation.

The Customer Security Management department performs the Security Officer registration process, while the technical provisioning (including changes to software, network provisioning, hardware, CUGs, MUGs and RBAC) is performed by other departments. A workflow system is used to help ensure that the necessary provisioning actions are taken.

Service activation can be started once the customer provisioning is completed. The actual technical provisioning process is largely automated to help ensure that provisioning requests are properly tracked, validated and reviewed during and after implementation.

Processes and procedures are in place to deactivate any SWIFTNet and FIN connections following the receipt of proper authorisation.

### 2.1.8. Message integrity

The integrity mechanisms at the transport layer include sender's SWIFTNet Link (SNL) to SWIFTNet and user-to-user integrity protection. The integrity of the messages sent between users and SWIFT (end-to-SWIFT) are verified by mandatory use of a PKI-based digital signature for InterAct, FileAct and MI Channel. This signature, also known as the authenticating signature, is calculated on the header and business data (known as payload) within the message and detects whether the message or file has been modified. User-to-user integrity protection is always used for MI Channel and is optional for InterAct and FileAct traffic.

The optional non-repudiation service (NRS) provides users with further verification of the origin and content of a SWIFTNet message. Non-repudiation processing is designed to provide users access to data that can be used to obtain certainty with regard to the authenticity of the origin, the emission of the message (or file), and optionally the reception of the message (or file).

Each FIN message carries a checksum to detect unauthorised modification. The message checksum is verified by each FIN processor that the message passes through. In addition, the integrity of authenticated

messages can also be verified by checking the PKI signature. The user-to-user authentication allows users to verify the integrity of information and the identity of the sender, independently of SWIFT.

### 2.1.9. Message validation

Message validation at the level of SWIFTNet is optional. It allows the validation of the payload content of InterAct messages. Message validation is performed against a reference template as well as validating bank identifier codes (BICs) and currency codes. Use of message validation is defined by the Service Administrator and applies to all messages using that service or, optionally, is triggered message by message. If validation is unsuccessful, the message is rejected and the reason is transmitted to the sender. The reference templates used for validation are constructed and maintained by the SWIFT Standards department in co-ordination with the interested members of the business community.

FIN message validation helps ensure that messages are sent from, and received by, valid destinations. It also verifies that the message adheres to the FIN message standards and any usage restrictions that apply to the type of message. Automated checks are performed to detect whether messages have been duplicated, intercepted and modified, or inserted without proper authorisation. Sequence numbers on input messages, from users, as well as delivery attempts, to users, provide information to detect lost or duplicated messages. Checksum comparisons against the corresponding trailers help detect whether the message payload has been changed.

### 2.1.10. Defence in depth

Defence in depth is a key component of SWIFT's cyber defence efforts and has always been part of the SWIFT security culture. This is demonstrated through a variety of controls covered in the various sections of this document. The controls include amongst others: monitoring of cyber threat information and security threat landscape analysis, anti-virus measures, security baselines and systems integrity monitoring, firewalls and network segmentation, intrusion detection, strong authentication and multi-layered encryption, security risk assessments and intrusion testing, incident and crisis management procedures, including cyber recovery exercises, as well as the incorporation of security measures in the software development lifecycle (for example code reviews and secure coding guidelines).

### 2.1.11. Change management process

The Change Management Process provides a formal mechanism for preparing, approving, tracking and implementing changes. This process is applicable to changes to existing and new products and services in the production environment.

SWIFT maintains two SWIFTNet environments: the integration testbed (ITB) environment and the production environment. The ITB allows SWIFT's Partners and software developers, including market infrastructures and other service providers, to test their SWIFTNet-based applications prior to deployment. ITB is not included in the scope of this report. The production environment supports the deployment of a tested application for users, either in a pilot trial or as a live operational service. The production environment is independent of the ITB environment.

### 2.1.12. Capacity management process

Capacity Planning is aimed at minimising the impact of system availability and performance issues and optimising the total cost of ownership of the enterprise computing infrastructure.

The assurance that the infrastructure is operating with adequate available capacity is obtained by the analysis of a collection of system's and traffic performance metrics. For this purpose the relevant systems are instrumented to regularly feed a performance data warehouse, which is also complemented with traffic monitoring extracted from application logs. The behaviour of the various systems is analysed at a frequency related to their criticality. Pertinent observation artefacts are produced at ad hoc frequency for sharing purpose, to provide evidence and to track the eventual follow-up actions linked to capacity shortage or issues.

A long term capacity plan is produced for SWIFTNet and FIN, which consists of an integrated workload model provided from Finance, the expected system capacity as per application development targets, tested in benchmarks and verified in production through performance analysis, and the various operational, resilience and procurement constraints. The plan, aligning the demand and supply side of systems deployment for several months or years, is then approved by the Capacity Clearance Committee for budgeting and further execution.

# 2 Information Security

### 2.1.13. Project lifecycle framework

SWIFT uses a methodology developed internally called ENCOMPASS (End-to-end Common Overview Method for Products and Services at SWIFT) to manage the development and delivery of products and services for both internal and external customers. This framework provides guidance for the product lifecycle, from concept through to product retirement, as well as the standards, procedures and guidelines for the preparation of deliverables.

A subset of the ENCOMPASS methodology and deliverables are mandatory depending on the type of project. Adherence to the mandatory components of the ENCOMPASS methodology is verified for selected projects by the Methodology & Controls team within Product. Adherence to this methodology directly supports quality, allowing a reduction in the number and severity of incidents.

ENCOMPASS ensures early and active involvement of security experts in a number of security touch points, specifically at the time of investment decisions, high level design and specification phases as well as during lower level design activities. Threat landscape, security classification, security specifications and risk assessments are examples of artefacts developed by these security experts.

Within Product, SWIFTNet/Market Infrastructure testing team and FIN testing are responsible for confirming that software functionality meets requirements and, to the extent possible, is defect-free.

### 2.1.14. Agile based lifecycle framework

The Agile Control Framework is a set of activities that must be performed to support business objectives, has been implemented for SWIFTNet Link and Alliance Gateway lifecycle.

Within this framework the product lifecycle is covered by squads being autonomous multidisciplinary teams enabled to define work and make business decisions. A squad is end-to-end responsible for the lifecycle, from product management, via change management, to deployment and problem management.

A rolling business plan is defined and maintained, reflecting the results of product delivery scope and priority alignment reviews as an input to or result from review meetings. Business requirements are identified, understood, prioritised and implemented to meet customer needs for releases going to a production environment. New and modified code goes through peer review to reduce the likelihood of defects and vulnerabilities prior to deliver the code change into a production environment.

The software is version controlled to ensure coherence of developed, tested and deployed software and track changes when packaging solutions for delivery into test and production environments.

Software integrity checks are implemented to give assurance that the software developed, built, tested and deployed was not altered when transferring packages to different environments. Security tests are conducted to confirm that the implemented changes meet the security baseline prior to releasing in a production environment. Personnel performing testing are independent from operational teams and perform their tests on a dedicated network and systems.

# 2 Information Security

## 2.2. Control objectives

The following control objectives govern a series of controls applied to information security for the SWIFTNet and FIN services:

1. Security measures (including logical access) to protect confidentiality and integrity of data are implemented;
2. SWIFT processes personal data of its customers in line with documented service commitments;
3. Customer authorised configuration changes are validated and implemented in accordance with the requests;
4. Cryptographic methods are designed and used to protect the confidentiality of customers' messages;
5. Mechanisms are in place to prevent and detect corruption of messages;
6. Changes are planned, validated and authorised prior to implementation;
7. Physical access to premises, computer equipment and resources is restricted;
8. Only authorised customers can access messaging services and messages are delivered to authorised recipients only.

The sections hereafter describe the different controls in place to meet each of these objectives.

### 2.2.1. Information security management

Control objective: Security measures (including logical access) to protect confidentiality and integrity of data are implemented.

Note: Controls 2.2.1.9, 2.2.1.16 and 2.2.1.27 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| 1. | Processes and procedures are implemented to review every two years whether standard cryptographic algorithms and corresponding key lengths used to provide security are appropriate for business purposes.<br><br>Every five years there is an independent review of proprietary cryptographic algorithms with a forecast to assess adequacy for the next five years. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the latest review of standard cryptographic algorithms and corresponding key lengths used to provide security to confirm that they have been reviewed within the last two years.<br>• Inspected the independent review documentation of proprietary cryptographic algorithms to confirm that no more than five years have elapsed |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | since the last review and the independent review covered a five years forecast.<br><br>**No relevant exceptions noted** |
| **2.** | Information security within SWIFT is the responsibility of the CEO and the Executive Committee, who act under the guidance and supervision of the Board. The Board meets multiple times a year to provide leadership in strategy, to decide on policy and to exercise proper supervision and control. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Terms of Reference and SWIFT Board Handbook to confirm that information security was within the responsibility of the CEO and the Executive Committee under guidance and supervision of the Board, and that providing leadership in strategy, deciding on policy as well as exercising supervision and control were Board's responsibilities.<br>• Inspect the composition of the Security Council to confirm that members of the Executive Committee were part of this Council.<br>• Inspect a sample of quarters to confirm that the Security Council discussed and supervised information security matters.<br><br>Reperformed, for all quarters, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, SWIFT IA's tests over the Terms of Reference and Handbook to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, SWIFT IA's tests over the Security Council to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **3.** | SWIFT has adopted an Information Security Control Framework (ISCF), based on guidance from ISO27001 and 27002 standards. The ISCF is approved by the CSO, and it defines the structure, hierarchy and interdependencies of Security Policies and Standards that define the security objectives and mandatory requirements. The ISCF consists of:<br>• SWIFT's Security Control Policy (SSCP) which lists control objectives for | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Information Security Control Framework to confirm that it was based on guidance from ISO27001 and 27002 standards, was approved by the CS, |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | ensuring the Confidentiality, Integrity, and Availability of customer messages; and<br>• SWIFT's Corporate Information Security Policy (SCISP) which establishes high level responsibilities related to the organisation of security, sets expectations for a culture of security, and describes the domain specific security policies and standards; along with a set of mandatory security techniques and measures to be adopted throughout the company. The SCISP is reviewed annually and is approved by the Security Council (SC), a security management committee consisting of all SWIFT ExCo members. It is chaired by the CEO and the CSO functions as its secretary. The SC meets at least four times a year. Minutes are produced from each meeting.<br>• Domain specific security policies and standards, covering the areas of security classification and ownership, operational security, system and software acquisition, development and maintenance, identity and access management, physical security, patch and vulnerability management, and cryptography. These policies are approved by the Security and Reliability Committee (SRC), the primary management body for oversight of the definition, implementation and improvement of the ISCF.<br>Deviations from security policies are managed according to the corporate security exception process and are subject to formal approval. | defined the hierarchy and interdependencies of Security Policies and Standards and consisted of SSCP and SCISP.<br>• Inspect the SCISP to confirm that it contained the requirements per the control, was annually reviewed and approved by the Security Council.<br>• Inspect a sample of quarters to confirm that the Security Council was consisted of all SWIFT ExCo members and that the SC discussed and supervised information security matters.<br>• Inspect specific security policies and standards to confirm that these were approved by the Security and Reliability Committee.<br>• Inspect a sample of deviations to confirm that these ware managed according to the corporate security exception process and were subject to approval.<br>**No relevant exceptions noted** |
| **4.** | The Global Security department:<br>• oversees the effectiveness of security of the messaging service infrastructure, physical locations, people and information;<br>• maintains the SWIFT Information Security Control Framework and monitors compliance; and<br>• manages corporate security issues. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT Information Security Control Framework to confirm that the Global Security department was responsible for overseeing security effectiveness, maintaining the security framework and monitoring compliance. |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | • Inspect a sample of identified corporate security issues to confirm that the Global Security department addressed the issues and managed the related risks.<br><br>**No relevant exceptions noted** |
| **5.** | SWIFT conducts background pre-employment and pre-assignment screening, which is subject to local laws and regulations, and is applicable to all new SWIFT employees and temporary SWIFT personnel with access to SWIFT locations and/or systems. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect global screening policy to confirm that the procedures were in line with the control description.<br>• Inspect for a sample of new SWIFT employees and temporary SWIFT personnel, the supporting documentation to confirm that the pre-employment and pre-assignment screening procedures were performed.<br><br>**No relevant exceptions noted** |
| **6.** | All SWIFT employees are requested to read and acknowledge understanding of the SWIFT Code of Conduct on a periodic basis. This includes understanding it is their responsibility to report a security issue if they suspect or have knowledge of possible violation of the SWIFT Code of Conduct or related policies. The SWIFT Code of Conduct stipulates that non-compliance or wilful violations of the SWIFT Code of Conduct or related policies may result in disciplinary action in accordance with appropriate procedures in each country. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect whether SWIFT employees are requested to read and acknowledge their understanding of the SWIFT code of conduct on a periodic basis.<br>• Inspected the latest published Code of Conduct to confirm it contained the clauses per the control description.<br><br>**No relevant exceptions noted** |
| **7.** | Software delivery and security functions are segregated to maintain independent oversight.<br><br>The following functions are performed outside of the software delivery teams in the production environment:<br>• Cyber Detection and Response;<br>• Security Compliance; and<br>• Identity and Access Management for Customer and Internal access. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected that accesses to all tools supporting the following functions were segregated from Software Delivery users in the production environment:<br>• Cyber Detection and Response;<br>• Security Compliance; and<br>• Identity and Access Management for Customer and Internal access<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **8.** | New SWIFT employees, contractors and consultants go through a security awareness training. Global Security promotes security awareness throughout the year through emails, articles and Human Intrusion Testing exercises. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of new SWIFT employees, contractors and consultants to confirm that they went through a security awareness training.<br>• Inspect the communication and exercises on security awareness to confirm that these were in place per the control.<br>**No relevant exceptions noted** |
| **9.** | SWIFT's Security Validation Program covers relevant targets within:<br>• IT infrastructure, including operating systems, network components and middleware;<br>• Scenario based or targeted red team exercises;<br>• Staff and contractor's response to simulated social engineering attacks;<br>• Scenario based table top exercises, including SOC capabilities.<br>As documented in the Security Validation Program Process, critical systems are tested annually, systems with lower criticality are tested at least every three years; those systems with the lowest criticality are tested on an ad-hoc basis. Processes are in place to ensure actions are taken to address issues identified. | Inquired with management to ascertain that the control operated as described.<br>Inspected the Security Validation Program to confirm that the following targets were covered:<br>• IT infrastructure: including operating systems, network components and middleware;<br>• Applications: including review of application source code, before and after deployment;<br>• Scenario based or targeted red team exercises;<br>• Staff and contractor's response to simulated social engineering attacks; and<br>• Scenario based table top exercises, including SOC capabilities.<br>Inspected a sample of systems to confirm that security validation was performed in line with their criticality.<br>Inspected a sample of security validation activities to confirm that actions were taken to address the identified issues.<br>**No relevant exceptions noted** |
| **10.** | Vulnerabilities identified for COTS and Open Source products are identified through scanning and intelligence feeds at least monthly. These vulnerabilities are evaluated for potential impact to SWIFT applications and services. Vulnerabilities are assigned a priority and possible remediation actions are identified. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of hosts to confirm that vulnerabilities were identified through vulnerability scanning and intelligence feeds, which operate across all technologies on a monthly basis. |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Security updates are installed in line with the requirements defined in SWIFT's Standards for Security Patching. Patching prioritisation is based on vulnerability severity and exposure of the system. | Inspected a sample of identified vulnerabilities to confirm that a priority and possible remediation actions were assigned based on their possible impact to SWIFT.<br><br>Inspected SWIFT's Standards for Security Patching to confirm that patching prioritization was based on the vulnerability severity and exposure of the system.<br><br>Inspected a sample of hosts, per technology, to confirm that security updates were installed in line with the requirements in SWIFT's Standards for Security Patching.<br><br>**Exceptions noted:**<br><br>We noted that:<br><br>1. For 3 out of 35 sampled hosts, vulnerability scanning was not performed within the frequency specified by SWIFT's processes.<br>2. For 8 out of 115 sampled hosts, security updates were not installed within the time limits specified by SWIFT policies. |
| **11.** | SWIFT has processes and procedures in place to identify and manage security threats:<br><br>• Public information about security and cyber threats is monitored daily (weekdays) and assessed for response by the Cyber Fusion Centre team through the usage of specialized intelligence portals offered by contracted providers and open source analysis.<br><br>• Global Security liaises with government and industry bodies to gather, distribute, assess information about cyber threats, cyber resilience objectives and practices. Frequency of meetings, calls or written updates is determined by the industry bodies involved.<br><br>• A process for the identification, assessment, mitigation, closure horizon, tracking and reporting of security risks is defined;<br><br>• The Board is informed at least on a yearly basis and more frequently as required of changes in the SWIFT security threat landscape and about SWIFT's security risks;<br><br>• Regular exercises are conducted as defined in the Cyber Attack Recovery | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the Cyber Fusion Centre to confirm that information about security and cyber threats was monitored and assessed for response.<br><br>• Inspect meeting minutes of meetings with government and industry bodies to confirm that Global Security liaised with them to gather, distribute, assess information about cyber threats, cyber resilience objectives and practices.<br><br>• Inspect the Information Security Risk Management documentation to confirm that risk assessments were performed to identify, assess, mitigate, track and report security risks.<br><br>• Inspect Board meeting minutes and agenda to confirm the Board was at least annually informed of SWIFT's security threat landscape and security risks.<br><br>• Inspect a sample of Cyber Attack exercises to confirm they were |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Plan to test effectiveness of cyber prevention, detection and response capabilities. | conducted as defined in the Cyber Attack Recovery Plan.<br>Reperformed, for a sample of Cyber Attack exercises, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, SWIFT IA's tests over the Cyber Fusion Centre and Information Security Risk Management documentation to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, SWIFT IA's tests over the Global Security meeting minutes to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **12.** | On an annual basis SWIFT conducts a review of its cyber maturity in selected areas. The review results are reported to the Security Council. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the 2020 Cyber Security Assessment and Roadmap to confirm that a review of cyber maturity in selected areas was performed and that the results were reported to the Security Council.<br>**No relevant exceptions noted** |
| **13.** | Identified and reported deviations from mandatory security practices or management acceptance of security audit issues are managed according to the corporate security exception process in which the residual risks are assessed and assessments are formally approved. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of identified and reported deviations from mandatory security practices to confirm that Global Security managed the deviations according to the corporate security exception process.<br>**No relevant exceptions noted** |
| **14.** | Four cyber security levels for SWIFT are defined:<br>• Baseline;<br>• Guarded;<br>• Elevated; and<br>• Critical.<br>Additional actions (e.g. additional staffing, faster escalation, more information sharing, additional | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Security Alert Management and Recovery for Cyber Security procedures to confirm that the required cyber security levels for SWIFT centres were defined. |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | hunting and increased reporting) are triggered by the increase of threat levels. | • Inspected the Security Alert Management and Recovery for Cyber Security procedures to confirm that additional actions have been defined in case of increase of threat level.<br><br>Reperformed for the Security Alert Management and Recovery for Cyber Security procedures, SWIFT IA's inspection over the procedures examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **15.** | SWIFT's Cyber Fusion Centre continuously monitors SWIFT's PROD environment.<br><br>Cyber Alerts are classified/prioritized and activities related to its investigation are logged as part of the ticket. In-depth investigation required for true positives (or at that moment unknown false positives) is documented and summarized before closure. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of hosts to confirm that these were monitored by the SWIFT Cyber Fusion Centre.<br><br>Inspected a sample of Cyber Alerts to confirm that they were classified and prioritized, and that investigation was performed.<br><br>Inspected a sample of true positive Cyber Alerts to confirm that in-depth investigation was performed and documented before closure.<br><br>**No relevant exceptions noted** |
| **16.** | Logical access to messaging service and swift.com's infrastructure components (both systems as well as network elements) is controlled via approvals according to defined procedures and level of access required.<br><br>Access is further subject to access rules for user-identification and password combinations. Primary accounts that provide access to SWIFT networks are revoked when SWIFT staff or contractors leave the company. Account lifecycle maintenance follows defined procedures.<br><br>Access to systems and network elements is reviewed and/or revoked upon a confirmed change in user functional roles and responsibilities according to defined account lifecycle procedures. Persistent access with no change in roles and responsibilities is reviewed biennially. Access that is deemed unnecessary is removed. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected that logical Access to the messaging service and swift.com's infrastructure was controlled with approvals based on documented procedures and the level of access required.<br><br>Inspected the configuration of access rules to confirm that access was subject to user-identification and password combinations.<br><br>Inspected a sample of staff or contractors joining SWIFT to confirm that their user access was approved according to the defined procedures.<br><br>Inspected a sample of SWIFT staff or contractors that left SWIFT, to confirm that their primary accounts that provide access to SWIFT networks were revoked.<br><br>Inspected a sample of hosts to confirm that persistent access was reviewed biennially and that unnecessary access was removed.<br><br>**No relevant exceptions noted** |
| **17.** | The team who performs source code management controls the access to programme source libraries and distributes new releases. | Inquired with management to ascertain that the control operated as described. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Software sources and changes are identified in the version control tool. Primary access to the source control systems is removed upon leaving. | Inspected a sample of new access requests to confirm that the access request was approved by appropriate management.<br><br>Inspected a sample of SWIFT staff or contractors that left SWIFT, to confirm that their primary access to the source control systems were revoked.<br><br>Inspected a sample of changes to confirm that software sources and changes were identified in the version control tool.<br><br>**No relevant exceptions noted** |
| **18.** | Passwords for privileged accounts must be transferred to and controlled by the Identity and Access Management group after system deployment. All accounts are documented for each particular service. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of hosts deployed to confirm that privileged accounts of systems and devices were transferred and controlled by the Identity Management group after system deployment using the TPAM tool.<br><br>Inspected a sample of hosts deployed to confirm that that each privileged accounts was documented for each particular service.<br><br>Inspected that only members of the Identity and Access Management group can manage passwords of privileged accounts.<br><br>**Exceptions noted**<br><br>We noted that for 2 out of 30 sampled hosts:<br><br>1. On 1 host, the password of a privileged account was not transferred to and controlled by the Identity and Access Management group after system deployment.<br>2. On 1 host, the audit trail demonstrating that privileged accounts were onboarded in the Identity and Access Management system after system deployment, was not available. |
| **19.** | Password-protected screensavers are automatically activated on Windows workstations after a pre-set period of inactivity. Monitoring workstations residing in computer rooms and Central Control Centres where screensavers would interfere with their operational purpose are excluded. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of Windows hosts to confirm that password-protected screensavers were automatically enforced after a pre-set period of inactivity.<br><br>Inspected the Group Policy on Active Directory level to confirm that the configuration of the password protected screensaver was enforced for SWIFT Windows Hosts.<br><br>**Exceptions noted** |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | We noted for 14 out of 30 sampled workstations:<br>1. On 8 out of 30 workstations it could not be confirmed that the global policy related to password-protected screensavers was enforced as the workstations were decommissioned.<br>2. On 6 out of 30 workstations, the global policy related to password-protected screensavers was not enforced. |
| **20.** | Firewall rules and access control lists implemented on the Production LAN hosting the messaging service infrastructure to segregate it from all other networks, including any local zone infrastructures, are reviewed on a sampling basis annually. Changes to firewall rules require a request from the business flow owner and approval from Global Security. The firewall rules and access control lists include those implemented on the Production LAN for segmentation to provide additional security. | Inquired with management to ascertain that the control operated as described.<br>Inspected the documentation on the Production LAN and other networks, the sampling based review by management and a sample of firewall rules and control lists to confirm that the Production LAN hosting the messaging services infrastructure was segregated and segmented from other networks.<br>Inspected a sample of firewall rule changes to confirm that a request from the business flow owner and global security was required.<br>**No relevant exceptions noted** |
| **21.** | In addition to the controls over user access to network elements, as per the Logical Access Control procedure, access to SWIFT's production networks is controlled through the secure configuration of switches and routers, in accordance with security policies and baselines. Access control lists and firewalls further restrict traffic flows to those that have been duly authorised. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of switches and routers to confirm that security configurations were in accordance with security policies and baselines.<br>Inspected a sample of access control lists to confirm that traffic flows were restricted to those that have been duly authorised.<br>Inspected a sample of firewalls to confirm that traffic flows were restricted to those that have been duly authorised.<br>**No relevant exceptions noted** |
| **22.** | Traffic sent between operating centres and traffic sent between remote BAPs and operating centres is encrypted at network line level. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of communication lines between operating centres and between remote BAP's and operating centres, to confirm that control existed and was operated as described.<br>**No relevant exceptions noted** |
| **23.** | Production privileged account passwords are managed according to defined requirements for length, complexity, change on use, and adhering to a minimum change frequency when unused. | Inquired with management to ascertain that the control operated as described.<br>Inspected that privileged account passwords rules defined in the production environment were managed according to defined requirements. |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | Inspected for a sample of hosts whether the passwords of its defined privileged accounts were managed according to the defined requirements on length, complexity, change on use and a minimum change on use when unused.<br><br>**Exceptions noted**<br><br>For 1 out of 35 sampled production hosts the minimum password change frequency requirement was not enforced for a production privileged account. |
| **24.** | SWIFT's Cyber Fusion Centre receives internal data feeds from different sources including network intrusion detection systems, web application firewalls, anti-virus, and operating systems logs (Unix, Windows and RHEL) based on documented prioritization that align with the Use Case process of the SOC. These feeds are compared with pre-defined logic to detect and alert anomalous activities. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the configuration and observed live data feeds of the monitoring tool used by SWIFT's Cyber Fusion Centre to confirm that for a sample of network elements and operating system the SWIFT Cyber Fusion Centre received the logs from these network elements and operating system.<br><br>Inspected a sample of use cases to confirm that data feeds were based on documented prioritization provided by the Security Operations Centre (SOC).<br><br>Inspected a sample of use cases to confirm that feeds were compared with pre-defined logic to detect and alert anomalous activities.<br><br>**No relevant exceptions noted** |
| **25.** | SWIFT has implemented network security controls for Internet-facing services and systems above the regular network security controls. These network security controls are DDoS protection, DMZ, reverse proxies, and Web Application Firewalls (WAF). | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the network security controls to confirm that DDoS protection, DMZ, reverse proxies and Web Application Firewalls were implemented.<br><br>Inspected a sample of internet facing services and systems to confirm that network security controls were applied.<br><br>**No relevant exceptions noted** |
| **26.** | Security baselines stipulate configuration requirements for server and workstation operating systems. These baselines define operating system level controls that include:<br><br>• Directories and file protection; and<br><br>• Logging and auditing.<br><br>Acceptance testing verifies security baseline compliance of tested releases. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the security baselines to confirm that these stipulated configuration requirements as well as operating system level controls.<br><br>Inspected a sample of releases to confirm that security baseline compliance was verified in the acceptance testing. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Security baseline compliance is verified for the production environment at least twice a year, with the exception of the verification of network routers and switches, which is performed yearly. Any deviations are identified and followed up through to resolution via a change request or waiver. | Inspected a sample of hosts to confirm that security baseline compliance was verified at least twice a year or yearly for network routers and switches and that identified deviations were followed-up through a change request or waiver.<br>**Exceptions noted**<br>For 8 out of 30 sampled workstations and servers, the security baseline compliance was not verified during the bi-annual checks. |
| **27.** | The SWIFT.com infrastructure is protected from the internet using multiple layers of firewalls and reverse proxies. The network infrastructure supporting SWIFT.com includes intrusion detection systems. SWIFT.com firewall security and intrusion detection events are monitored 24/7. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect SWIFT.com network and SWIFT.com infrastructure documentation, to confirm that SWIFT.com was protected from the internet through the use of multiple layers of firewalls and reverse proxies, and that SWIFT.com was protected through the use of an Intrusion Detection System.<br>• Inspect the firewall and intrusion detection configuration to confirm that firewall security alerts and intrusion alerts were monitored 24/7.<br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |
| **28.** | Standard SWIFTNet security is implemented using three independent security layers between customer premises and SWIFT operating centres as follows:<br>• Network layer: all traffic between the customer VPN box and the SIPN BAP-VPN tunnel concentrators, over the Network Partner IP networks, is sent over encrypted IP tunnels;<br>• Information transfer layer:<br>– Message communication between the customer's SWIFTNet Link and the SWIFTNet front end processor at a SWIFT OPC is encrypted;<br>– Message communication between the customer's SWIFTNet Link or MFP and the | Inquired with management to ascertain that the control operated as described.<br>Inspected results of management's test on non-production environment to confirm that management ascertained that SNL was starting successfully only when configured to support encrypted messages.<br>Inspected results of management's test on non-production environment to confirm that management ascertained that non encrypted T2S messages sent from SNL will be automatically encrypted by the SNL.<br>Inspected results of management's test on non-production environment to confirm that management ascertained that SNL cannot decrypt messages not addressed to it.<br>Inspected results of management's test on non-production environment to confirm that |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | MI Channel Gateway at a SWIFT OPC is encrypted;<br>– Message communication between the customer's AGI and the Instant Switch at a SWIFT OPC is encrypted;<br>– Browse and SWIFT WebAccess traffic between the customer component, SWIFT components and the service provider's Web server, as applicable, is encrypted by the Transport Layer Security (TLS); and<br>• Application layer: where selected by customer, encryption of InterAct messages between customers based upon SWIFTNet certificates.<br>Direct Internet SWIFT WebAccess traffic is encrypted using TLS and does not use standard SWIFTNet Network layer encryption. | management ascertained that a valid certificate was used to encrypt by TLS the Direct Internet SWIFT WebAccess traffic.<br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **29.** | The generation of the SWIFTNet CA private root keys is performed according to an audited root key generation procedure. SWIFTNet CA root keys are renewed according to predefined intervals.<br>The CA uses tamper-resistant hardware devices (FIPS level-3 compliant) for additional protection of the root key. It is also protected by fully monitored dual access controlled cages. | Inquired with management to ascertain that the control operated as described.<br>Inspected the generation of the SWIFTNet CA private root keys to confirm that this was performed according to an audited root key generation procedure and that key renewal was performed according to predefined intervals.<br>**No relevant exceptions noted** |
| **30.** | SWIFT encrypts the payload of all SWIFTNet messages flagged for non-repudiation before they are archived. SWIFT also encrypts the payload of all SWIFTNet customer-to-customer messages and files stored within the Store-and-Forward (SnF) system.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br>Inspected the results of management's test on non-production environment to confirm that management ascertained that payload of SWIFTNet archived messages flagged for non-repudiation were encrypted.<br>Inspected the results of management's test on non-production environment to confirm that management ascertained that payload of SWIFTNet customer-to-customer messages and files archived within the SnF system were encrypted.<br>Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| | **FIN Specific** | |

# 2 Information Security

## 2.2.1 Information security management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **31.** | SWIFT encrypts user-to-user FIN messages before they are stored. System messages with user payload are also encrypted before they are stored (such as the MT 021).<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages were not readable when stored.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages containing user payload were not readable when stored.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages were encrypted.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages (type MT021 and MT086) containing user payload were encrypted.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.2. Personal data protection

Control objective: SWIFT processes personal data of its customers in line with documented service commitments.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | The SWIFT Personal Data Protection Policy and Data Retrieval Policy govern the protection of personal data processed by SWIFT in the provision of its services.<br><br>The SWIFT Personal Data Protection Policy also contains specific provisions regarding the responsibilities and accountabilities of customers for the protection of personal data since effective control over personal data are significantly dependent on controls exercised by those customers. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect SWIFT Personal Data Protection Policy and Data Retrieval Policy to confirm that these policies governed the protection of personal data processed by SWIFT in the provision of its services.<br>• Inspect SWIFT personal Data Protection Policy to confirm that it contained specific provisions regarding the responsibilities and accountabilities of customers for the protection of personal data.<br><br>Reperformed, for the SWIFT Personal Data Protection Policy and Data Retrieval Policy, SWIFT IA's inspection tests over the policies examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **2.** | The messaging services SWIFTNet & FIN are organized to operate in multiple zones, a European (EU) zone and a Transatlantic (TA) zone, and support both intra-zone traffic and inter-zone traffic. Under normal operating conditions SWIFTNet and FIN process and store all EU intra-zone production traffic within the SWIFT operating centres located in Europe. For synonym based FIN traffic, the processing and storage zone(s) are determined by the country code of the sender and receiver master destinations. The inter-zone traffic between the EU and TA zones may be globally processed and stored. SWIFT WebAccess, SWIFTNet store-and-forward and MI Channel application components are hosted only in the EU zone. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of daily traffic reports to confirm that messaging services SWIFTNET & FIN were organised to operate in multiple zones and that intra-zone and inter-zone traffic were processed per the control.<br><br>Inspected SWIFT WebAccess, SWIFTNet store-and-forward and MI Channel application components to confirm that they were only hosted in the EU zone.<br><br>**No relevant exceptions noted** |
| **3.** | All BICs with the same country code belong to the same zone.<br><br>The following processes are implemented to ensure that zone membership changes are properly authorised and implemented: | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the Country to zone allocation configuration and change process document to confirm that processes are implemented as described in the control. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | • A formal zone membership request needs to be received from the National Membership Group (NMG) of the respective country or from the country's user community (if there is no formal NMG); and<br>• The provisioning of the country and zone relationship is subject to verifications and is performed subject to the four eyes principle. | Inspected for a sample of membership change requests to confirm they were handled as described in the control.<br>**No relevant exceptions noted** |
| **4.** | Routing based on BIC attribute by the SNL is in place to prevent global zone traffic from being routed to a local zone infrastructure and local zone traffic from being routed to the global zone infrastructure.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspected the results of management's test on non-production environment to confirm that management ascertained that messages routed from another local zone infrastructure were not received by the SNL.<br>• Inspected the results of management's test on non-production environment to confirm that management ascertained that messages to another BIC routed from global zone infrastructure were not received by the SNL.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **5.** | A Privacy Officer is appointed to oversee compliance with the SWIFT Personal Data Protection Policy and the Ad Hoc Contract between SWIFT SCRL and its US branch for the personal data transfers in SWIFT messages that pass from the EU to the TA messaging zone.<br>Oversight of compliance is achieved by means of a combination of the following activities: maintenance of data processing activities register, ad hoc risk analysis, training and specific arrangements in the incident handling process regarding personal data breach. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT organisation chart to confirm that a Privacy Officer was appointed.<br>• Inspect SWIFT Personal Data Protection Policy and reports on Data Protection Policies, to confirm that compliance was achieved through maintenance of data processing activities register, ad hoc risk analysis, training and specific |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | arrangements in the incident handling process regarding personal data breach.<br><br>**No relevant exceptions noted** |
| **6.** | For collective exceptional requests, as per the SWIFT Data Retrieval Policy, procedures are in place to:<br>• Review and assess the justification of the requestor that the request is legitimate;<br>• Notify the requesting organisation or authority of the confidential nature of the data and request them to preserve this confidentiality; and<br>• Ensure the aggregation and anonymisation of the provided data. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the SWIFT Data Retrieval Policy to confirm that procedures are in place to handle collective exceptional requests as described in the control.<br><br>Inspected a sample of collective exceptional requests received by SWIFT to confirm that the requests were handled as described by the process.<br><br>**No relevant exceptions noted** |
| **7.** | For mandatory exceptional requests, as per the SWIFT Data Retrieval Policy, procedures are in place to:<br>• Review the documentation provided by the third party to demonstrate the legitimacy of their request for the retrieval of traffic or message data. This is part of the process to authorise the execution of such requests;<br>• Notify the requesting authority of the confidential nature of the data, SWIFT's obligation to inform its customers, and any other protections that may apply to the data. SWIFT will also request the competent authority to preserve the confidentiality and any other protections of the data; and<br>• Inform customers that have sent or received data which is included in such mandatory retrieval, unless prevented by applicable law, as acknowledged by the Board or its delegated body. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the SWIFT Data Retrieval Policy to confirm that procedures are in place to handle mandatory exceptional requests as described in the control.<br><br>Inspected a sample of mandatory exceptional requests received by SWIFT to confirm that the requests were handled as described by the process.<br><br>**No relevant exceptions noted** |
| **8.** | SWIFT does not use customer messages for testing purposes unless permitted by SWIFT's Data Retrieval Policy. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT's data retrieval policy to confirm that customer messages could not be used for testing purposes unless permitted by the policy. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | • Inspect the FIN Message Extract Process description to confirm that the process included CSM to provide a decryption token.<br>• Inspect the CSM on-call guide to confirm that CSM was reviewing the legitimacy of the request an informed the privacy officer before providing the decryption token.<br>• Inspect the password recovery mechanism for the software which generated the decryption token to confirm that the password was stored in a central repository system with approval rules to access it.<br>**No relevant exceptions noted** |
| **9.** | System dumps can contain message transaction data. Such data is available for a limited period and accessible to problem management staff on a need-to-have basis, and operational procedures are in place to control access to such data. System logs do not contain customers' message transaction data.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br>Inspected the results of management's test on non-production environment to confirm that management ascertained that customer's message transaction data could not be written to system log files of SWIFTNet and FIN.<br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>Inspected a sample of systems to confirm that message transaction data was available for a limited period of time.<br>Inspected the access provisioning process to confirm that access to system dumps was assigned on a need-to-have basis.<br>**No relevant exceptions noted** |
| **10.** | Any given country is allocated to only the European (EU) zone or the Transatlantic (TA) zone for the messaging services SWIFTNet & FIN. Messages that are not intended to contain personal customer information may be processed and stored outside of the originating zone; for example, Test & Training messages, forex confirmation messages. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of countries connected to the SWIFT Messaging Services SWIFTNet & FIN to confirm that they were assigned to either the European or the Transatlantic zone.<br>**No relevant exceptions noted** |
| **11.** | The messaging solutions using copy services may have intra-zone messages being copied to a third party located in another zone. For transparency purposes, SWIFT publishes the concerned third party copy service relationships | Inquired with management to ascertain that the control operated as described. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | on swift.com for FINInform-based services. For other copy services, participants can contact the service administrators if they want to know which messages will get copied and to which BICs. | Inspected www.swift.com to confirm that third party copy service relationships for FINInform-based services were published.<br><br>Inspected the implemented process and system configurations to confirm that SWIFT could look up a Copy service and disclose the third party which received the copy messages when requested by an authorised party.<br><br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |
| **12.** | The SNL establishes independent connections to the TA and EU zones.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SNL had two independent connections to the TA and the EU zones.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that messages from the TA zone reached the SNL through the TA connection.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that messages from the EU zone reached the SNL through the EU connection.<br><br>• Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.3. Customer configuration management

Control objective: Customer authorised configuration changes are validated and implemented in accordance with the requests

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | To ensure that only the Service Administrator can request emergency updates, SWIFT authenticates the Service Administrator via the secure channel on swift.com. | • Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of emergency updates to confirm that the requestor of each emergency updates was a valid Service Administrator that was authenticated via exchanged passwords or via the secure channel on swift.com.<br>**No relevant exceptions noted** |
| **2.** | Customer configuration changes are tracked and subject to a number of manual and automatic validations (such as mandatory fields and data formats) to ensure that they are complete and appropriately authorised. The validation controls are documented.<br>Configuration actions are documented in procedures, with critical procedures clearly marked. | Inquired with management to ascertain that the control operated as described.<br>Inspected customer configuration procedures to confirm that these contained the requirements per the described control.<br>Inspected for a sample of customer configuration changes that they were validated and authorised before being implemented.<br>**No relevant exceptions noted** |
| **3.** | SWIFT has automated tools, processes and procedures to ensure changes to closed user groups (CUGs) and Message User Groups (MUGs) are authorised.<br>For the set-up of a market infrastructure or MA-CUG, the request for the setup needs to be initiated by the Service Administrator by sending a duly signed Service Approval Request Form (SARF) and Service Administration Agreement to SWIFT.<br>SWIFT management validates and approves the market infrastructure or MA-CUG requests. The Board is informed of the setup of new market infrastructures through a written report.<br>Changes to MUG membership result from a change in SWIFT user category or the registration to additional SWIFT services.<br>SWIFT implements changes to the service profiles of market infrastructure- or MA-CUGs upon instructions from their Service Administrators. The user, the Service | Inquired with management to ascertain that the control operated as described.<br>Inspected the detailed Service Creation Modification and Termination Process documents which defined the requirement of approvals necessary for a service creation or any request affecting the services (Modification/termination) to confirm that these documents were aligned with the control.<br>Inspected a sample of market infrastructure or MA-CUG set-ups to confirm that the request was initiated by the Service Administrator through duly signed Service Approval Request Form (SARF) and Service Administration Agreement, that the request was validated and approved by SWIFT management and that the Board was informed.<br>Inspected a sample of modified or terminated MUGs / CUGs / MA-CUGs to confirm that the modification or termination was performed per |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Administrator or SWIFT can request the withdrawal of a user from a market infrastructure or MA-CUG. The validation process uses internal procedures and checklists. | the request (SPF), and that the validation was done per internal procedures and checklists.<br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **4.** | Processes and procedures exist to ensure that SWIFT performs administration for validated and approved FINCopy CUGs to take effect following a Maintenance Window, when the information is received from the authorised Service Administrator at least 14 days before the required update time. | Inquired with management to ascertain that the control operated as described.<br>Inspected the procedures and system configuration in place to confirm that the required administration was facilitated for validated and approved FINCopy CUGs to take effect following a Maintenance Window, when the information is received from the authorised Service Administrator at least 14 days before the required update time.<br>**No relevant exceptions noted** |
| **5.** | For FIN, message usage restrictions applicable to users are approved by the Board and implemented through specific MUGs. FIN MUGs can also be used to define the message types allowed (such as the MT 204) between a certain group of users. | Inquired with management to ascertain that the control operated as described.<br>Inspected process documentation to confirm that message usage restrictions applicable to users required Board approval and implementation through specific MUGs.<br>Inspected the system configuration to confirm that FIN MUGs could be used to define message types allowed between certain groups of users.<br>Inspected a sample of MUG message requests to confirm that these were approved by the Board.<br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.4. Encryption

Control objective: Cryptographic methods are designed and used to protect the confidentiality of customers' messages.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Traffic sent between operating centres and traffic sent between remote BAPs and operating centres is encrypted at network line level. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of communication lines between operating centres and between remote BAP's and operating centres, to confirm that control existed and was operated as described.<br><br>**No relevant exceptions noted** |
| **2.** | Private keys associated with SWIFTNet certificates are stored in an encrypted PKI profile, to which access is protected by a password.<br><br>Profiles used to sign live customer-to-customer FIN messages, must be stored in a Hardware Security Module (HSM), a tamper-resistant hardware device.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the results of testing performed by management on non-production environment to confirm that management ascertained that private keys associated with certificates used for authentication of customers, integrity and confidentiality of customer messages were stored in a secure location, when relevant an HSM, and that procedures and processes were in place for the storing of private keys.<br><br>Inspected the results of testing performed by management on non-production environment to confirm that management ascertained that messages will not be sent in case and incorrect password was entered or no login was possible in case the certificate was removed.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **3.** | InterAct, FileAct and FIN enforce a password selection policy for private key passwords based on a minimum length and a number of other syntax rules.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected results of testing performed by management on non-production environment to confirm that management ascertained that InterAct, FileAct and FIN enforced password settings based on a minimum length and a combination of other syntax rules for a private keys.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **FIN Specific** | |
| **4.** | SWIFT encrypts user-to-user FIN messages before they are stored. System messages with user payload are also encrypted before they are stored (such as the MT 021).<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages were not readable when stored.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages containing user payload were not readable when stored.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages were encrypted.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages (type MT021 and MT086) containing user payload were encrypted.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |
| **5.** | SWIFT encrypts the payload of all SWIFTNet messages flagged for non-repudiation before they are archived. SWIFT also encrypts the payload of all SWIFTNet customer-to-customer messages and files stored within the Store-and-Forward (SnF) system.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that payload of SWIFTNet archived messages flagged for non-repudiation were encrypted.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that payload of SWIFTNet customer-to-customer messages and files archived within the SnF system were encrypted. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **6.** | The Customer Security Management department (CSM) analyses critical events generated by the SWIFTNet CA and creates a trouble ticket to track problems until resolution. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the processes and procedures defined to confirm that the Customer Security Management department needed to analyse critical events generated by the SWIFTNET CA and in case of problems needed to create a trouble ticket.<br><br>Inspected for a sample of weeks, the weekly generated list of critical events by the SWIFTNet, to confirm that CSM analysed these critical events, created trouble tickets for identified problems and resolved these tickets.<br><br>**No relevant exceptions noted** |
| **7.** | Customer certificates used for Instant, InterAct and FileAct are renewed according to predefined intervals. The certificate renewal is triggered:<br>• For InterAct and FileAct when a customer application successfully logs into the profile.<br>• For Instant automatically.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that if a customer certificate was in the predefined renewal interval, the certificate was renewed:<br>• when the customer successfully logged into InterAct or FileAct; or<br>• automatically for certificates used for Instant.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **8.** | Standard SWIFTNet security is implemented using three independent security layers between customer premises and SWIFT operating centres as follows:<br>• Network layer: all traffic between the customer VPN box and the SIPN BAP-VPN tunnel concentrators, over the Network Partner IP networks, is sent over encrypted IP tunnels;<br>• Information transfer layer: | Inquired with management to ascertain that the control operated as described.<br><br>Inspected results of management's test on non-production environment to confirm that management ascertained that SNL was starting successfully only when configured to support encrypted messages.<br><br>Inspected results of management's test on non-production environment to confirm that management ascertained that non encrypted |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | – Message communication between the customer's SWIFTNet Link and the SWIFTNet front end processor at a SWIFT OPC is encrypted;<br>– Message communication between the customer's SWIFTNet Link or MFP and the MI Channel Gateway at a SWIFT OPC is encrypted;<br>– Message communication between the customer's AGI and the Instant Switch at a SWIFT OPC is encrypted;<br>– Browse and SWIFT WebAccess traffic between the customer component, SWIFT components and the service provider's Web server, as applicable, is encrypted by the Transport Layer Security (TLS); and<br>• Application layer: where selected by customer, encryption of InterAct messages between customers based upon SWIFTNet certificates.<br>Direct Internet SWIFT WebAccess traffic is encrypted using TLS and does not use standard SWIFTNet Network layer encryption.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | T2S messages sent from SNL will be automatically encrypted by the SNL.<br>Inspected results of management's test on non-production environment to confirm that management ascertained that SNL cannot decrypt messages not addressed to it.<br>Inspected results of management's test on non-production environment to confirm that management ascertained that a valid certificate was used to encrypt by TLS the Direct Internet SWIFT WebAccess traffic.<br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **9.** | The generation of the SWIFTNet CA private root keys is performed according to an audited root key generation procedure. SWIFTNet CA root keys are renewed according to predefined intervals.<br>The CA uses tamper-resistant hardware devices (FIPS level-3 compliant) for additional protection of the root key. It is also protected by fully monitored dual access controlled cages. | Inquired with management to ascertain that the control operated as described.<br>Inspected the generation of the SWIFTNet CA private root keys to confirm that this was performed according to an audited root key generation procedure and that key renewal was performed according to predefined intervals.<br>Inspected the root keys' protection mechanisms in place to confirm that these were implemented and operated as described.<br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.5. Message and system integrity

Control objective: Mechanisms are in place to prevent and detect corruption of messages

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **1.** | SWIFT has procedures in place to isolate a local zone infrastructure from the SWIFT global network. These procedures would be exercised in extreme cases where a malicious compromise or unforeseen behaviour is detected in the local zone hardware or software potentially impacting SWIFT global services. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the operational procedure documents to confirm that SWIFT had procedures in place to isolate a local zone infrastructure from the SWIFT global network.<br>• Inspect the outcome of an isolation test to confirm that the test was successful.<br>Reperformed, for the operational procedure documents and outcome of an isolation test, SWIFT IA's tests over the documents and test examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **2.** | To detect the corruption of messages, a checksum (CHK) trailer is added to messages to allow the FIN system and the interface to check messages for corruption and transmission errors. If a message is corrupted it is rejected with a Negative User Acknowledgement reply to the sender.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FIN messages contained a CHK trailer.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that corrupted or changed messages did not have the same CHK as the original message.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that a message with a different computed CHK than the CHK trailer was rejected and a Negative User Acknowledgement message was shared with the sender.<br>• Inspect that management documented the basis for determining that non-production environment used for |

| | | |
|---|---|---|
| | | application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **3.** | The SWIFT Offline Message Accountability (SOMA) application reconciles FIN messages against delivery histories and verifies no gaps exist in input or output sequence numbers.<br><br>In addition, Inter-SP FINCopy Reconciliation (inter-SP FCR) process reconciles MT097's exchanged between SPs where FINCopy server and emitter BIC are on different SPs.<br><br>A periodic process called FINCopy Verifier (FCV) verifies the following for all messages selected for FINCopy or FINInform services:<br>• That all messages requiring approval from Service Administrators are copied (MT 096);<br>• That all authorisations/refusals received from the Service Administrator (MT 097) are processed; and<br>• That all authorised messages have been queued for delivery to the receiver.<br><br>SOMA, FCR and FCV generate daily event and exception information (tickets). These events are monitored daily. Exceptions are escalated to Level 2 support for further investigation and are formally tracked. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that SOMA reconciled FIN messages against delivery histories and reconciled input and output sequence numbers.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FCR reconciled MT097 messages exchanged between SPs with different BICs.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FCV validated that MT096 was copied.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that FCV validated that MT097 was processed.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that authorised message was queued for delivery.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that SOMA, FCR and FCV generated tickets for identified exceptions.<br>• Inspect a sample of daily integrity checks to confirm that follow-up of identified integrity check issues was performed in line with escalation requirements.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |

| | | |
|---|---|---|
| **4.** | SWIFT maintains a secure system and procedures to verify non-repudiated messages. To enable this:<br>• Hardware, software, message backups and audit trails which are required are maintained for at least the retention period; and<br>• Public keys, certificate status changes and all other information required to verify the signatures are backed up and are securely stored and managed by SWIFT.<br>Specifically, the following is archived:<br>• All requests to the CA issued by Security Officers, and all SWIFT responses;<br>• All offline requests to Customer Security Management, issued by Security Officers, and all SWIFT responses;<br>• All changes to the status of entities; and<br>• All valid and expired or revoked certificates.<br>Certificate status can be determined for at least six months after private key expiry or revocation. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described<br>• Inspect the policies and procedure documents to confirm that SWIFT maintained a secure system and procedures to reverify non-repudiated messages.<br>• Inspect the backup and retention configuration and implemented practices to confirm that public keys, certificate status changes, and other information required to verify signatures were backed up, securely stored and maintained for at least the retention period.<br>• Inspect on a sample basis the archiving to confirm the following was archived:<br>– All requests to the CA issued by Security Officers, and all SWIFT responses;<br>– All offline requests to Customer Security Management, issued by Security Officers, and all SWIFT responses;<br>– All changes to the status of entities; and<br>– All valid and expired or revoked certificates.<br>• Inspect the certificate configuration to confirm that the certificate status could be determined for at least six months after private key expiry or revocation.<br>**No relevant exceptions noted** |
| **5.** | SWIFTNet messages flagged for non-repudiation are time stamped by the SWIFTNet Switch. The re-verification process assesses that the certificate was valid at the time of processing of the message. This time message is based on the time stamp at the SWIFTNet Switch.<br>These messages are grouped in files, which are signed by the non-repudiation process to allow detection of corruption during archival by verifying the signed files.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br>Inspect results of management's test on non-production environment to confirm that management ascertained that non-repudiation flagged messages were time stamped by the SWIFTNet Switch.<br>Inspect results of management's test on non-production environment to confirm that management ascertained that the re-verification process on a message using a valid was successful.<br>Inspect results of management's test on non-production environment to confirm that |

| | | |
|---|---|---|
| | | management ascertained that an attempt to process a message using a revoked, expired or forged certificate was detected by the re-verification process.<br><br>Inspect results of management's test on non-production environment to confirm that management ascertained non-repudiation flagged messages were grouped in files before archiving.<br><br>Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to archive a set of messages containing at least one corrupted was detected by the non-repudiation process.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **6.** | In order to detect the corruption of messages sent from the sender to SWIFT, SWIFTNet validates end-to-SWIFT signatures on the signed data of every message.<br><br>Optionally, SWIFT provides the mechanism so the customer can sign end-to-end, which can be used to detect corruption at the application level. SWIFT will centrally check if end-to-end signing is mandatory and that traffic is compliant with the selected service attributes (end-to-end signature, signature format).<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the end-to-SWIFT signatures on the signed data for messages sent to SWIFT.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that messages with non-compliant end-to SWIFT signatures were not processed by SWIFTNet.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the end-to-end signatures on the signed data for messages sent to SWIFT if end-to-end signing was activated.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.6. Change management

Control objective: Changes are planned, validated, and authorised prior to implementation.

Note: Controls 2.2.6.1, 2.2.6.5, 2.2.6.6, 2.2.6.7, 2.2.6.8 and 2.2.6.9 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | SWIFT applies a formal change implementation process for all change requests to hardware and software. All change requests are subject to change implementation rules, as defined in the process. Change requests are formally documented in a change record and subject to approval of the relevant approving authority. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of changes to confirm that these were documented, formally tracked and approved by the relevant approving authority as defined in the formal change implementation process.<br>**No relevant exceptions noted** |
| **2.** | Operating procedures are reviewed as defined in the documented process. Changes to the procedures are formally approved. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the workflow supporting the release of operating procedures to confirm that operating procedures were reviewed as defined in the documented process, and that the updated operating procedures were approved prior to publication.<br>**No relevant exceptions noted** |
| **3.** | Software is released upon authorised request and integrity verification is performed on releases of SWIFT-produced messaging software as part of the deployment process for production systems. | Inquired with management to ascertain that the deployment process control operated as described.<br>Inspected a sample of releases of SWIFT-produced messaging software to confirm that an integrity check was performed as part of the deployment process, and that the release was |

| | | |
|---|---|---|
| | | performed upon an authorised request and approval thereof.<br><br>**No relevant exceptions noted** |
| **4.** | The team who performs source code management controls the access to programme source libraries and distributes new releases. Software sources and changes are identified in the version control tool. Primary access to the source control systems is removed upon leaving. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of new access requests to confirm that the access request was approved by appropriate management.<br><br>Inspected a sample of SWIFT staff or contractors that left SWIFT, to confirm that their primary access to the source control systems were revoked.<br><br>Inspected a sample of changes to confirm that software sources and changes were identified in the version control tool.<br><br>**No relevant exceptions noted** |
| **5.** | The development methodology defines standards for functional requirements specification, design specification and testing, which can be verified by quality assessments, quality transition checkpoints and product testing.<br><br>The required evidence is reviewed and approved by the relevant stakeholders as per the development methodology. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect development lifecycle methodology to confirm that standards for functional requirements, design specification and testing were defined.<br><br>• Inspect a sample of projects to confirm that these projects applied the development methodology.<br><br>**Exceptions noted**<br><br>We noted that the design specification was reviewed but not approved prior to deployment for 1 out of 11 sampled SWIFTNet software releases that were deployed in production. |
| **6.** | Developers attend mandatory secure coding training, as per policy with a refresher training performed every 3 years. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the SATE (Security Awareness, Training, and Education) policy to confirm that developers needed to attend a mandatory secure coding training with a refresher every 3 years.<br><br>• Inspect a sample of developers to confirm that they attended mandatory secure code training per the SATE policy. |

| | | |
|---|---|---|
| | | Reperformed, for a sample of developers, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the SATE policy, SWIFT IA's tests over the policy examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **7.** | Peer level code review is performed on code related to the main message flow and security functions. Records are kept to document findings from code reviews as well as corrective actions. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Code Review Procedure to confirm that peer level code review was needed on code related to the main message flow and security functions.<br>• Inspect a sample of changes to the main message flow and security functions to confirm that peer level code review was performed, and identified findings were documented together with the corrective actions.<br><br>Reperformed, for a sample of changes, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the Code Review Procedure, SWIFT IA's tests over the procedure examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **8.** | Secure coding standards are based on OWASP and SANS 25 CWE (software errors) and reviewed regularly. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the secure coding standards in use to confirm that these were based on OWASP and SANS25 CWE, and were reviewed regularly.<br><br>Reperformed, for the secure coding standards, SWIFT IA's tests over the coding standards examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |

| | | |
|---|---|---|
| **9.** | New and modified code for programming languages commonly used in SWIFT developed applications is scanned by a Static Analysis Security Tool.<br><br>For SWIFT developed applications, web-based Graphical User Interfaces are evaluated by a Dynamic Analysis Security Tool. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the Code Review Procedure to confirm for SWIFT developed applications that new and modified code for commonly used programming languages required scanning by a Static Analysis Security Tool, and that web-based Graphical User Interfaces required evaluation by a Dynamic Analysis Security Tool.<br><br>• Inspect a sample of changes to SWIFT developed applications to confirm that scanning of new and modified code for commonly used programming languages as well as evaluation to the web-based Graphical User Interfaces were performed.<br><br>Reperformed, for a sample of changes to SWIFT developed applications, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the Code Review Procedure, SWIFT IA's tests over the procedure examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **10.** | A Test Strategy defines the types of tests to be executed, before releasing a new product version (e.g. regression testing, logical intrusion testing, functional testing, performance testing, pilot testing).<br><br>Exit Criteria, aiming at achieving the expected level of quality prior to releasing the new version, are documented in the Test Strategy. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect a sample of releases to confirm that a test strategy and exit criteria were defined and documented.<br><br>Reperformed, for a sample of releases, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **11.** | For major new services, operational readiness tests (ORT) verify SWIFT's operational capability. Test results are documented and actions are tracked. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described. |

| | | |
|---|---|---|
| | | • Inspect the procedure supporting project management to confirm that operational readiness tests (ORT) was required for major new services.<br>• Inspect a sample of major new services to confirm that an operational readiness test was performed and documented.<br>**No relevant exceptions noted** |
| **12.** | With the exception of emergency releases, regression testing of software releases is performed before they are deployed on the production systems. For emergency releases, regression testing of any changed functionality is incorporated in the next release. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the procedure supporting the release process to confirm that requirements on regression testing were included.<br>• Inspect a sample of releases to confirm that regression testing was performed prior to deployment on the production systems.<br>• Inspect a sample of emergency releases to confirm that regression testing of any changed functionality was incorporated in the next release.<br>**No relevant exceptions noted** |
| **13.** | SWIFT's Cyber Fusion Centre receives internal data feeds from different sources including network intrusion detection systems, web application firewalls, anti-virus, and operating systems logs (Unix, Windows and RHEL) based on documented prioritization that align with the Use Case process of the SOC. These feeds are compared with pre-defined logic to detect and alert anomalous activities. | Inquired with management to ascertain that the control operated as described.<br>Inspected the configuration and observed live data feeds of the monitoring tool used by SWIFT's Cyber Fusion Centre to confirm that for a sample of network elements and operating system the SWIFT Cyber Fusion Centre received the logs from these network elements and operating system.<br>Inspected a sample of use cases to confirm that data feeds were based on documented prioritization provided by the Security Operations Centre (SOC).<br>Inspected a sample of use cases to confirm that feeds were compared with pre-defined logic to detect and alert anomalous activities.<br>**No relevant exceptions noted** |
| **14.** | SWIFT's Cyber Fusion Centre continuously monitors SWIFT's PROD environment.<br>Cyber Alerts are classified/prioritized and activities related to its investigation are logged as part of the ticket. In-depth investigation required | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of hosts to confirm that these were monitored by the SWIFT Cyber Fusion Centre. |

| | | |
|---|---|---|
| | for true positives (or at that moment unknown false positives) is documented and summarized before closure. | Inspected a sample of Cyber Alerts to confirm that they were classified and prioritized, and that investigation was performed.<br><br>Inspected a sample of true positive Cyber Alerts to confirm that in-depth investigation was performed and documented before closure.<br><br>**No relevant exceptions noted** |
| **15.** | The deployment process outlines deliverables and quality requirements to be met before deployment into the production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Operations Deployment process document to confirm that the deployment process outlined deliverables and quality requirements to be met before deployment into the production environment.<br>• Inspect a sample of projects to confirm that quality requirements were met before deployment into the production environment.<br><br>Reperformed, for a sample of projects, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the Operations Deployment process document, SWIFT IA's tests over the process examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **16.** | SWIFT maintains a software product inventory, including COTS and Open Source, which are authorized for usage. The availability of vendor support for COTS products is annually reviewed. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected that the Commercial Off-The-Shelf baseline was maintained by SWIFT, governing the authorised usage in a release.<br><br>Inspected a sample of COTS products to confirm that the availability of vendor support was reviewed on an annual basis.<br><br>**No relevant exceptions noted** |
| **17.** | Anti-virus software is installed and virus signatures are kept up to date on Windows workstations and servers to prevent and detect the presence of known virus/malware.<br><br>The usage of USB devices on the Windows physical workstations and Thin Clients is restricted. Deviations on the usage of USB | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the central configuration of USB access restrictions for production |

| | | |
|---|---|---|
| | devices is authorised as per process through a maintained list with the granted exceptions.<br><br>Non-compliant systems are identified and reported to system owners and line management for follow-up. | workstations to confirm that manual data transfer via USB was restricted.<br>• Inspect a sample of Windows physical workstations and Thin Clients to confirm that deviation on the usage of USB devices was authorized and documented.<br>• Inspect a sample of Windows workstations and servers to confirm that anti-virus software was installed and signature files were kept up to date.<br>• Inspect a sample of antivirus alerts and USB alerts, to confirm that follow-up was performed and that Non-compliant systems were identified and reported.<br><br>**Exceptions noted:**<br><br>For 5 out of 30 sampled production Windows workstations and servers, the anti-virus signatures were not kept up to date. |
| **18.** | SWIFT staff are authorised to use operational commands via defined roles and profiles. Based on an approval process, internal user accounts are assigned to these roles and profiles. Their roles and profiles are documented per service. Shared accounts are used within the Operating and Central Control Centres to facilitate monitoring and control. Outside of the Operating and Central Control Centres generic accounts are prohibited except by explicit permission. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the processes and procedures to confirm that SWIFT staff required approval to use operational commands and that internal user accounts were assigned to these roles and profiles.<br><br>Inspected a sample of shared accounts with operational commands assigned, to confirm that these were authorised.<br><br>**Exceptions noted:**<br><br>We noted that the audit trails related to explicit permissions of the use of shared accounts outside the Operating and Central Control Centres that were set-up prior to the period in scope, were not available. |
| **19.** | There are software integrity checking mechanisms in place on the SWIFTNet and FIN messaging production systems. These mechanisms regularly verify the integrity of the key executables and configuration files. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of hosts in scope, to confirm that the integrity checking mechanism was installed and performed integrity checks.<br>• Inspect a sample of weekly integrity check reports to confirm that follow-up of the identified discrepancies was performed. |

| | | |
|---|---|---|
| | | **Exception noted:**<br>We noted that 4 out of 25 sampled FIN and SWIFTNet production messaging systems were not monitored for software integrity. |
| | **SWIFTNet Specific** | |
| **20.** | SWIFT designs and tests the APIs of new mark releases of SWIFTNet Link to ensure backward compatibility with the previous mark release. | Inquired with management to ascertain that the control operated as described.<br>Inspected result of regression testing performed by management on non-production environment to confirm that management ascertained that APIs of new mark releases were compatible with the previous mark release.<br>Inspected that management documented the basis for determining that non-production environment used for regression testing was adequate.<br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **21.** | SWIFT has a process in place for emergency FIN Copy update and withdrawal operations within 45 minutes as documented in the FIN Copy Service Description. | Inquired with management to ascertain that the control operated as described. We were informed that there were no emergency FIN Copy update and withdrawal requests during the examination period.<br>Inspected the processes and procedures related to emergency FIN Copy updates and withdrawal to confirm that these required execution of emergency FIN copy update and withdrawal operations within 45 minutes.<br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.7. Physical access

Control objective: Physical access to premises, computer equipment and resources is restricted.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Physical security protection mechanisms are in place to restrict access to SWIFT-owned Operating Centres (OPC) and CCCs to SWIFT personnel and other specifically authorised individuals. These protection mechanisms consist of:<br>• fences;<br>• closed circuit TV security monitoring;<br>• 24x7 guard force;<br>• baggage scanning;<br>• metal detectors;<br>• mantraps;<br>• Emergency exits from OPCs are alarmed to notify of entry or exit.<br>The physical security of leased BAPs, OPCs and CCC area is monitored, via CCTV and intrusion detection alarm, from the SWIFT owned and operated CCCs. | Inquired with management to ascertain that the control operated as described.<br>Observed the SWIFT owned OPCs and CCCs to confirm that the physical protection mechanisms were in place.<br>Observed the physical security monitoring dashboards at the CCCs to confirm that remote monitoring of the physical security protection mechanisms in the leased data centres and leased CCCs was in place.<br>**No relevant exceptions noted** |
| **2.** | The SWIFT facilities are divided into security zones for which different physical access controls are defined and applied. The SWIFT facilities access control systems are maintained and updated to limit access to security zones as per the Physical Security Policy.<br>Manned and unmanned computer rooms, containing production networks and systems, are within dedicated areas supported by restricted access control.<br>A periodic review of access permissions to the different security zones is done by SWIFT. | Inquired with management to ascertain that the control operated as described.<br>Inspected the SWIFT facilities to confirm that:<br>• SWIFT facilities were divided into security zones for which different physical access controls were defined and applied;<br>• access control systems were maintained and updated to limit access to the security zone per the Physical Security Policy; and<br>• computer rooms containing production networks and systems were within dedicated areas supported by restricted access controls.<br>Inspected relevant documentation to confirm that a periodic review of access permission to different zone was performed.<br>**No relevant exceptions noted** |
| **3.** | The guard force is responsible for the protection of the operating centres, including: | Inquired with management to ascertain that the control operated as described. |

# 2 Information Security

## 2.2.7 Physical access (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | • Monitoring the physical security of the site;<br>• Facilitating visitor access to and from the OPC; and<br>• Handling security and safety incidents, including reporting and escalation.<br><br>For leased standalone BAP and CCC facilities, physical security protections are in place, but are not under the direct control of SWIFT. SWIFT security alarms are monitored remotely by the CCCs. | Inspected the guard schedule to confirm that the guard force had a 24/7 presence onsite at SWIFT owned facilities operating centres.<br><br>Inspected the guard's checklist on ServiceNow to confirm that the guard force was responsible for:<br>• monitoring the physical security of the sites;<br>• facilitating visitor access to and from the OPC; and<br>• handling security and safety incidents, including reporting and escalation.<br><br>Observed the physical security monitoring dashboards at the CCC's to confirm that security alarms for standalone BAPs and CCCs were monitored remotely.<br><br>**No relevant exceptions noted** |
| **4.** | Four security levels for physical access to the operating centres are defined:<br>• Baseline<br>• Guarded<br>• Elevated<br>• Critical<br><br>Access restrictions and additional checks are triggered by the increase of threat levels. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the Type – 4 Facility Security Level Definition procedures document to confirm that the required security levels for physical access to the operating centres were defined.<br><br>**No relevant exceptions noted** |
| **5.** | BAPs are designed and operated to SWIFT specifications and are continuously monitored by control staff. These specifications include at least the following:<br>• Access control using access tokens;<br>• Closed Circuit TV security monitoring;<br>• Intrusion detection system. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the CCTV footage inside the guard room to confirm that the cameras for the BAP locations were monitored<br><br>Inspected a sample of BAP entry control reports to confirm that access and intrusions were monitored.<br><br>**No relevant exceptions noted** |
| **6.** | The Media Sanitisation Standard mandates the sanitisation methods for highly confidential or confidential information (e.g. wiping, degauss).<br><br>Media (such as disk drives or tape cartridges) containing highly confidential information are not taken offsite for maintenance or repair. These media are securely disposed of by overwriting, reformatting or physical destruction to help ensure that no data can be retrieved from these media. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the Media Sanitisation Standard to confirm that sanitisation methods for highly confidential or confidential information were mandated.<br><br>Observed the operating centres to confirm that media was sanitised in line with the procedures |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Media destruction can be performed offsite by certified destruction companies in compliance with relevant standards regarding secure destruction of confidential material.<br><br>SWIFT premises are equipped with shredders to accommodate safe disposal of sensitive documents. | detailed in the standard and operating procedures.<br><br>Observed that SWIFT premises were equipped with shredders to accommodate safe disposal of sensitive documents.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.8. Message access management

Control objective: Only authorised customers can access messaging services and messages are delivered to authorised recipients only.

Note: Controls 2.2.8.3 and 2.2.8.4 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | SWIFT registers two SWIFTNet security officers as part of the onboarding process, each receives an individual secure code card. Requests from registered SWIFTNet security officers are only acted upon after successful authentication of the requesting security officer(s), using their secure code card. Secure channel authenticates the security officers as part of request creation, if the request includes credentials to return, these credentials are protected by a password that are only known by the security officer. | Inquired with management to ascertain that the control operated as described.<br>Inspected the procedure used to setup the Security Officers access.<br>Inspected that for a sample of authorized customers, two SWIFT Net security officers were registered.<br>Inspected that the secure code card corresponding to the initial provisioning requests were activated by the initial security officers for each institution provisioned with the messaging services.<br>Inspected that the credentials could only be recovered through Secure channel after the proper authentication steps involving the SCC cards were taken.<br>**No relevant exceptions noted** |
| **2.** | SWIFT deactivates a customer upon authorised request from the customer as requested in the order form or by SWIFT in certain circumstances (such as revoked banking licence, non-payment, non-compliance with admission criteria or violation of Terms and Conditions). | Inquired with management to ascertain that the control operated as described.<br>Inspected the deprovisioning flow to confirm it stipulated the procedures, approvals and requirements necessary for the deactivation of a BIC.<br>Inspected a sample of customer deactivations to confirm that these were supported by a request from the customer or from SWIFT.<br>**No relevant exceptions noted** |
| **3.** | The CSM department verifies that in order to access SWIFTNet, each customer has registered at least two Security Officers (SOs) who are designated by the customer as those persons authorised to manage its PKI certificates and, | Inquired with management to ascertain that the control operated as described.<br>Inspected the procedure used to setup the Security Officers access. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | more generally, to communicate with SWIFT on all SWIFTNet security matters.<br><br>The initial Security Officers' identity and authority must be contractually confirmed.<br><br>A new security officer must first register on SWIFT.com. The SWIFT.com administrator approves the SWIFT.com registration request. | Inspected a sample of new SO requests to confirm that initial Security Officers' identity and authority was contractually confirmed and the SO requests was approved by SWIFT.com (SDC) administrator.<br><br>Inspected all the active institutions to confirm that at least two SOs were registered.<br><br>Inspected that the Secure Channel application did not allow for the registration with less than two SOs and did not allow the deletion of a SO if the total number of SOs would become less than two.<br><br>**No relevant exceptions noted** |
| **4.** | swift.com administrator accounts are created upon validation of a submitted registration form. Subsequently the swift.com administrators create their passwords themselves. Customer and administrator access to the protected area of www.swift.com is secured by a 2 step verification process as described on swift.com. After an initial 2 step verification, users can opt to trust their device and defer repeating the second step for up to 30 days. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the process descriptions on SWIFT.com to confirm that swift.com administrator account requests required validation via a registration form, and that access to the protected area of swift.com required a 2 step verification process.<br><br>Inspected the swift.com access configuration for the protected area to confirm that the access was secured by a 2 step verification process.<br><br>Inspected a sample of swift.com administrator account creations to confirm that the creation was performed upon receipt of a validated registration form.<br><br>Observed the configuration of swift.com to assess that users were able to opt to trust their device up to 30 days.<br><br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |
| **5.** | To connect to SWIFTNet, through MV-SIPN, a customer needs a VPN device whose serial number has been registered with SWIFT and a valid certificate, issued by the SIPN Certificate Authority (CA), to set up the IP-Sec VPN tunnels. SWIFT Backbone Access Points (BAPs) perform node authentication to verify that VPN tunnels that connect to SWIFT are certified. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquired with management to ascertain that the control operated as described.<br><br>• Inspect a sample of VPN connections for connecting to SWIFTNet through MV-SIPN to confirm that the customer had a VPN device whose serial number was registered with SWIFT and a valid certificate issued by the SIPN Certificate Authority (CA). |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | • Inspect SWIFT Backbone Access Points (BAPs) to confirm that node authentication was performed to verify that VPN tunnels that connect to SWIFT were certified.<br><br>**No relevant exceptions noted** |
| **6.** | SWIFT provides customers the ability to revoke their SWIFTNet messaging certificates through an online SWIFTNet service or an offline request to Customer Security Management via Secure Channel.<br><br>Management tests this control at least once annually. Where tests are performed in a test environment Management ensures the test environment is equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected results of testing performed by management on non-production environment to confirm that management ascertained that SWIFTNet messaging certificate could be revoked through an online SWIFTNet service.<br><br>Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>Inspected a sample of offline customer requests via Secure Channel, to confirm that the certificates were revoked timely.<br><br>**No relevant exceptions noted** |
| **7.** | Upon receipt of a customer request to revoke their SWIFTNet messaging certificates, the requestor is authenticated and its rights to perform revocation verified. When requested, an off-line certificate revocation request will be performed within 2 hours, after the successful authentication of the requesting customer Security Officer.<br><br>Any attempt to access SWIFTNet InterAct, FileAct and Instant is denied within 5 minutes of an on-line certificate revocation. Any attempt to authenticate a new SWIFT WebAccess session, is denied within 5 minutes of an on-line certificate revocation.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of customer revocation request to confirm that the requestor was authenticated and its rights to perform revocation were verified, and that the revocation was performed within 2 hours after successful authentication of the requesting customer security officer.<br><br>Inspected result of testing performed by management on non-production environment to confirm that management ascertained that access was denied within 5 minutes after the certificate used for the authentication was revoked online.<br><br>Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **8.** | To prevent the misuse of obsolete certificates and private keys, SWIFT has processes and procedures to revoke and disable the certificates of institutions that cease to be SWIFTNet users. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected a sample of institutions that ceased to be SWIFTNet users to confirm that certificates of these institutions were revoked or disabled.<br><br>**No relevant exceptions noted** |
| **9.** | The AGI, SNL and MFP are authenticated at connection time and access to the store-and-forward queues is controlled by the appropriate Role Based Access Control (RBAC) role containing the name of the queue.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that queues cannot be started if AGI, SNL or MFP were corrupted.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that RBAC roles were defined to protect access to each specific store-and-forward queue.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that without "access to the store-and-forward queues" RBAC roles, customer cannot launch commands using store-and-forward queues.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **10.** | SWIFTNet validates the status, scope of authority and role profile of Security Officers' certificates to help ensure only authorised Security Officers issue certificate management requests to SWIFT according to their defined roles.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that certificate management requests issued by Security Officers authenticated with revoked, expired or forged |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | certificate were not processed by SWIFT.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that certificate management requests out of the scope of the authority or role of the Security Officers issuer were not processed by SWIFT.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **11.** | To use the optional SWIFTNet store-and-forward (InterAct or FileAct) copy mechanism the service administrator must provide a third party DN list.<br>SWIFT has established and applies consistently a set of rules for processing a request on a service with a copy feature.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that an administrator with an invalid, incomplete or not related third party DN list was not able to use the optional SWIFTNet store-and-forward copy mechanism.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the set of rules defined by SWIFT for processing a request on a service with a copy feature was implemented.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **12.** | A SWIFT User can allow other SWIFT Users to initiate a Store-and-Forward retrieval request on their behalf by provisioning the appropriate RBAC role.<br>Retrieved messages are only delivered to the original sender (for an input retrieval request) or | Inquired with management to ascertain that the control operated as described.<br>Inspected the results of management's test on non-production environment to confirm that the message requested to be retrieved in an input retrieval request was delivered only to the original sender of the message. |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | original receiver (for an output retrieval request) of the message.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected the results of management's test on non-production environment to confirm that the message requested to be retrieved in an output retrieval request was delivered only to the receiver sender of the message.<br><br>Inspected the results of management's test on non-production environment to confirm that only authorized SWIFT user having the appropriate RBAC role can initiate a Store-and-Forward retrieval request.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **13.** | The message reception registry (MRR) contains the rules for routing messages to their destination. When MRR changes are requested by the customer, SWIFT authenticates the customer and validates the fact that the customer is authorised to access the rules of his organisation.<br><br>Customers can use different RBAC roles to segregate access to the reroute command between live and test environments.<br><br>The SNL provides fallback capabilities between multiple SNL instances, without SWIFT's intervention.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected results of testing performed by management to confirm that management ascertained that MRR changes cannot be requested by a customer not authenticated by SWIFT or not having access to the rules of his organisation.<br><br>Inspected results of testing performed by management to confirm that management ascertained that no single RBAC role allowed the access to the reroute command in live and test environments.<br><br>Inspected results of testing performed by management to confirm that management ascertained that customers could specify multiple SNL endpoints in the MRR to redirect traffic. Between these endpoints.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **14.** | Except for services available to the whole community (such as the SWIFTNet Online Operations Manager), access to Browse and SWIFT WebAccess is controlled via PKI and by checking that:<br><br>• for Browse, the SNL used by the customer is part of a IP-CUG or<br><br>• for SWIFT WebAccess, the user identity belongs to an institution BIC8 that is | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to connect to Browse using an IP |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | member of the SWIFT WebAccess service (Appl-CUG).<br><br>SWIFT requires that Browse and SWIFT WebAccess TLS sessions uses a certificate-based authentication mechanism.<br><br>Customers accessing SWIFT WebAccess services directly from the Internet need an activated personal token and a valid certificate issued by the SWIFTNet CA.<br><br>The certificate is used to set up a two-way authenticated TLS session.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | not part of the IP-CUG, was not successful.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to connect to SWIFT WebAccess using a user identity belonging to an institution BIC8 not part of the Appl-CUG, was not successful.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to connect to WebAccess using a revoked, expired, forged certificate or not issued by the SWIFTNet CA was not successful.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to connect to WebAccess without an activated personal token was not successful.<br>• Inspect results of management's test on non-production environment to confirm that management ascertained that an attempt to connect to WebAccess without an activated personal token was not successful.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **15.** | SWIFT applies formal procedures and audit trails for requests to retrieve SWIFTNet messages stored for non-repudiation.<br><br>The CSM department is responsible for performing the retrieval with the system enforcing dual authorisation to ensure two authorised individuals (an operator and an approver) perform the process.<br><br>For customers, the resulting information is sent according to their instructions. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected process and procedure documents to confirm that formal procedures and audit trails were applied for requests to retrieve SWIFTNet messages stored for non-repudiation.<br><br>Inspected the retrieval process documentation to confirm that dual authorisation was required and that resulting information should be sent according to customer's instructions.<br><br>**No relevant exceptions noted** |

# 2 Information Security

## 2.2.8 Message access management (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **16.** | The SWIFT Identity Provider (IdP) performs an authentication of the end-user on request of a configured SWIFT WebAccess service provider via a PKI signature.<br><br>Once an end-user is authenticated with a PKI signature, a session cookie is created that is valid for a limited period of time and can be used for authentication to SWIFT during that period.<br><br>When RBAC is configured for the SWIFT WebAccess service, the IdP validates that the end-user possesses at least one RBAC role for the service.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that an attempt to authenticate to SWIFT WebAccess using a revoked, expired or forged PKI was not successful.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a session cookie was created after a successful authentication on SWIFT WebAccess with a PKI signature.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that session cookie was created with an expiration time.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that with a valid and non-expired session cookie, no authentication was requested to access SWIFT WebAccess.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the user was entitled at least for one RBAC role for the service, if RBAC was configured for this service.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **17.** | The SWIFT Identity Provider (IdP) offers a non-repudiation (NR) service for SWIFT WebAccess service providers. If the service provider requests for NR by signing a request, the IdP requires the end-user to confirm and sign the transaction, which the IdP stores as evidence and informs the service provider. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | confirm that management ascertained that IdP required the confirmation of the transaction and the signature of the transaction when the service provider requested NR.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that IdP stored the confirmation and the signature of the transaction in case of NR request.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that IdP informed the service provider of the confirmation and the signature of the transaction in case of NR request.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **18.** | In order to activate personal tokens, used for accessing SWIFT WebAccess services directly over the Internet, the customers' security officer needs to securely collect activation secrets from SWIFT. The tokens used are FIPS 140-2 Level-2 compliant and are personalised by SWIFT before distribution to customers.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that an attempt to a validate personal token with an invalid activation code was not successful.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that an attempt to authenticate on SWIFT WebAccess services without a personal token code was not successful.<br>• Inspect the certification of tokens delivered by SWIFT to customers' security officers to confirm that they were at least compliant FIPS 140-2 L2 compliant.<br>• Inspect that management documented the basis for determining that non-production environment used for |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | | application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **19.** | There is mutual authentication of the customer and FIN by PKI signatures. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the authentication's configuration deployed on FIN to assess that authentication of customers on FIN were based on KPI signatures.<br><br>**No relevant exceptions noted** |
| **20.** | Customers can perform routine retrieval of their FIN messages via a specific system message (that is MT020).<br><br>Customers can also request SWIFT's CSM department to perform the retrieval on their behalf and have their retrieved messages sent according to their instructions. If such a request is submitted over the secure channel, CSM informs the Privacy Officer of the request. If the request is submitted through some other channel, CSM requires it to be authorised by the Privacy Officer.<br><br>The CSM department performs the retrieval of FIN messages during normal business hours (CET), using profiles that segregate the internal submitter and approver of the request. For retrievals requested outside of business hours, a separate approver is not required. However, all emergency requests are reviewed during the next business day.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described. We were informed that there were no customers retrieval requests during the examination period.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that the MT020 message retrieved FIN messages.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **21.** | FIN users may obtain access information that shows LT session histories and login attempts for the preceding 30 days.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained |

| Control Applied | Work Performed / Observations |
|---|---|
| | that LT sessions histories and login attempts were kept for 30 days.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a period of historical LT sessions and login attempts was defined.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FIN user could access historical LT sessions and login attempts.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **22.** Customer-to-customer message authentication procedures apply to FIN customers. The messages are authenticated by the receiver using the PKI signature added by the sender.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the customer-to-customer message authentication's configuration deployed on FIN to confirm that messages were authenticated by the receiver using the PKI signature added by the sender.<br>**No relevant exceptions noted** |
| **23.** In addition to FIN controls, FINCopy supports an additional mechanism:<br>• To allow the FINCopy Service Administrator to authenticate the sender of the original FIN message, of which it receives the copy; and<br>• To allow the FINCopy message recipient to authenticate that the FIN message is authorised by the FINCopy Service Administrator.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FINCopy allowed the Service Administrator to authenticate the sender of the original FIN message.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FINCopy allowed the message recipient to authenticate that the FIN |

| Control Applied | Work Performed / Observations |
|---|---|
| | message was authorised by the FINCopy Service Administrator.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **24.** There are checks that ensure that:<br>• The FIN customer-to-customer message is signed using a Hardware Security Module; and<br>• The signing authority of the message matches its sender.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspected result of testing performed by management on non-production environment to confirm that management ascertained that FIN customer-to-customer message was signed with certificates stored in an HSM.<br>• Inspected result of testing performed by management on non-production environment to confirm that management ascertained that FIN validated that the signing authority of the message matched with the sender authority.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.1. Introduction

This section describes how SWIFT implements appropriate policies and procedures, and devotes sufficient resources to ensure that our critical services are available, reliable, and resilient. It also explains how business continuity management and disaster recovery plans support the timely resumption of the critical services in the event of an outage in scope of this report.

### 3.1.1. SWIFTNet and FIN availability targets

The availability and resilience of the messaging service infrastructure is of prime importance to SWIFT users. SWIFTNet and FIN services are expected to be available to the user population in accordance with the goals set out in the Operational Performance Report. For 2020, overall FIN service weighted availability was targeted at 99.990%. SWIFTNet service weighted availability was targeted at 99.990%.

Weighted availability is calculated by multiplying the unscheduled service downtime with a weighting factor determined by a combination of historical traffic patterns (number of messages) and customer connections (per network node, or, for FIN, per regional processor). This is done to be able to reflect in a single overall service availability percentage, the impact of outages affecting only parts of the customer base or parts of SWIFT services.

### 3.1.2. Redundant architecture

The SWIFT messaging services are designed to be available 24 hours a day, 365 days a year, with some planned downtime. Customers are given advance notice of planned downtime per the Maintenance Windows.

SWIFT maintains operating centres (OPCs) on different continents to provide full site redundancy. In addition, within each OPC, the central systems are designed to eliminate single points of failure.

SWIFT has two OPCs for a given zone or zone-less service and each OPC can completely host the services by itself. Data is replicated between the two OPCs to avoid data loss in case of controlled actions or minimize data loss in case of disaster scenarios.

The systems and networks at each OPC are configured to allow them to meet the processing requirements of the SWIFT user community in the concerned global zone(s). This is not applicable to SnF since SnF is not zoned and is only present in the EU zone. Processes and procedures are in place to keep technical facilities in good order as well as to keep operational staff fully proficient.

SWIFT employs two redundancy models, the Active/Standby and Active/Active configurations:

- In the Active/Standby configuration a component is implemented on two processors and disks are shared between the processors (using a dual-ported RAID configuration). One processor is active, the other is idle and ready to take over; and a heartbeat mechanism is established between the systems. In most cases, the standby automatically takes over in case there is no heartbeat from the active system.
- In the Active/Active configuration the components are spread over independent physical boxes, each with their own disks. The underlying protocol specifically recognises the arrangement and load balances the traffic over the boxes. In case of failure of one box, the system is designed so that traffic is automatically redirected to the remaining boxes.

In both Active/Standby and Active/Active redundancy configurations, the remaining systems have adequate capacity to manage traffic at peak loads. The network topology is designed to have at least two separate routes that can carry the full traffic load between OPCs.

### 3.1.3. Operational monitoring

Technology Platform is responsible for the day-to-day monitoring of all critical aspects of the systems and networks within the OPCs. This group is divided into specialised teams and continuously monitors and controls the messaging service infrastructure. Two mechanisms are used to automate these activities:

- The operational management systems, which display software (application and operating system level) and hardware alerts, and events sent by the SWIFTNet and FIN messaging systems; and
- The network management systems, which display alerts and events sent by the network elements, and, at regular intervals, perform a polling of network critical components.

# 3 Reliability and resilience

SWIFT uses modelling tools to analyse and forecast systems capacity so that equipment and resources can be added when volumes increase beyond the tolerance of existing systems. Mechanisms that monitor system resources also alert operators of thresholds being exceeded.

### 3.1.4. Archiving and retention of data

Archival procedures and retention periods are based on the data archiving requirements of the different systems and services.

For FIN, messages are replicated between OPCs within a zone as a result of main message flow. FIN messages are also archived to long-term storage at OPCs to support data retrieval for 124 days.

Under normal operating conditions, only SWIFTNet messages and files sent in Store-and-Forward mode are replicated between OPCs. Information required for non-repudiation services is also replicated between OPCs within a zone for archiving purposes and available for 124 days, and this occurs within no more than 90 minutes.

### 3.1.5. Incident and crisis management

SWIFT uses a variety of channels including SWIFT.com, to inform customers of the status of the messaging service infrastructure. When a fault occurs, status updates are available to registered customers.

The online customer support service allows customers to search a knowledge base for known problems and workarounds. This information includes most frequently asked questions and answers, troubleshooting and diagnostic guidelines, and status reports about known problems. Furthermore, the customer may contact Global Support Delivery (GSD) to request assistance.

The Problem Management team within Technology Platform monitors and resolves problems encountered with the production systems and networks. Based on defined criteria, certain problems are escalated to the status of incidents (see the definition of *incident* in the Glossary).

Incidents require notification of the Command Centre, which coordinates incident follow-up and status reporting, and ensures notification to the relevant executives. Incidents are escalated to the CIO and a post-incident management review report (PIMR) is prepared.

For a crisis, a Crisis Management team is put in place according to an established process. This process defines the required reactions, depending on the nature and the type of the crisis.

SWIFT has defined disaster scenarios, for which plans are documented to mitigate various events and to continue operational activities from alternate locations. A yearly test plan helps ensure that critical areas of the messaging services infrastructure are covered by exercises to assess readiness.

The quarterly Operational Performance Report describes incidents and is reviewed by the Technology and Production Committee of the Board.

# 3 Reliability and resilience

## 3.2. Control objectives

The following control objectives govern a series of applied controls relating to reliability and resilience of the SWIFTNet and FIN services:

1. In the event of an outage, policies, procedures, and resources are in place to support the timely resumption of services in line with documented service commitments;
2. The messaging service infrastructure is designed to ensure the continuity of operations in line with documented service commitments;
3. Availability of the messaging services are monitored to detect and react to problems;
4. SWIFT has developed Business Continuity Plans and Disaster Recovery Plans in line with service commitments;
5. Processes and procedures are in place to ensure the messaging services infrastructure has sufficient capacity to process messages;
6. SWIFT validates messages, and only validated messages are processed and delivered.

The sections hereafter describe the different controls in place to meet each of these objectives.

### 3.2.1. Outages

Control objective: In the event of an outage, policies, procedures, and resources are in place to support the timely resumption of services in line with documented service commitments.

Note: Controls 3.2.1.3, 3.2.1.6, 3.2.1.7, 3.2.1.8 and 3.2.1.10 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| 1. | SWIFT operational activities are documented in procedures, with critical steps clearly marked. Critical steps are those operational activities where failure of the specified action could affect availability and activities performed on an infrequent basis. | Inquired with management to ascertain that the control operated as described.<br>Inspected documentation to confirm that SWIFT operational activities were documented in procedures, with critical steps clearly marked where failure of the specified action could affect availability and activities performed on an infrequent basis.<br>**No relevant exceptions noted** |
| 2. | Processes and procedures exist to ensure that SWIFT retains all available messages or other records the General Counsel requested to retrieve and preserve if a SWIFT user makes a valid claim regarding messages it sent or received, until instructed otherwise by the General Counsel. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described<br>• Inspect the procedures and process documentation to confirm that SWIFT |

| | | |
|---|---|---|
| | | retained and retrieved all messages or other records in case of a SWIFT user claim.<br><br>Reperformed, for the procedure and process documentation, SWIFT IA's tests over the documentation examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **3.** | At least one crisis exercise is conducted annually, unless the Crisis Team has been activated during the year, to evaluate the readiness and effectiveness of the Crisis Team. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Simulation Support Master Plan to confirm that it was planned to activate the Crisis Team at least annually, and that the Crisis Team was activated in the past year.<br><br>**No relevant exceptions noted** |
| **4.** | Based on defined retention periods and methods of disposal, non-customer data potentially used in the recovery of systems is backed up and stored. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the configuration of backups related to non-customer data to confirm that non-customer data was backed up and stored.<br>• Inspect monthly backup reports to confirm that retention period of non-customer data's backup were assigned as defined in the Retention Policy.<br><br>Reperformed, for the configurations of backups related to non-customer data and monthly backup reports, SWIFT IA's tests over the backups examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **5.** | At least once a year, SWIFT tests if SWIFTNet and FIN redundancies achieve disaster site takeovers within 20 minutes for a single Zone Site Take-over, and within 30 minutes for a concurrent Site Take-over in two Zones. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the annual test report to confirm that SWIFTNet and FIN redundancies achieved disaster site takeovers within |

| | | |
|---|---|---|
| | | 20 minutes for a single Zone Site Take-over, and within 30 minutes for a concurrent Site Take-over in two Zones.<br><br>Reperformed, for the annual test report, SWIFT IA's tests over the report to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **6.** | Certain problems are classified as incidents (as defined in Appendix A: Glossary). Incidents are subject to a post incident management review involving review by the Crisis Executive (CIO). | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT incident management manual and post incident management manual process documents to confirm that the control was designed as described.<br>• Inspect a sample of incidents to confirm that these were subject to a post incident management review involving the Crisis Executive (CIO).<br><br>**No relevant exceptions noted** |
| **7.** | The SWIFT.com environment is deployed in two sites. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the network maps and system locations to confirm that the procedures were in line with the control description.<br>• Inspect a sample of servers to confirm that they were configured in a resilient setup<br><br>**Exceptions noted**<br><br>We noted that 1 out of 3 sampled servers in the swift.com environment was only deployed at one site. |
| **8.** | Based on defined retention periods, SWIFT.com data is backed up and stored at an off-site location. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of SWIFT.com servers to confirm that these were backed up and stored at an off-site location in adherence to the defined retention |

| | | |
|---|---|---|
| | | periods, and that in case of backup failures a follow-up was performed.<br><br>**No relevant exceptions noted** |
| **9.** | Source code is replicated multiple times a day between SWIFT locations.<br><br>Backups of the systems and databases hosting the source code are performed daily and stored at a remote SWIFT location. Successful completion of backups is monitored on a daily basis and restore tests of the backups are performed on an annual basis. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inspect the configuration of the replication deployed for SWIFT source code repositories to confirm that source code was replicated multiple times a day between SWIFT locations.<br><br>• Inspect the configuration of backups for a sample of systems and databases hosting source code hosts to confirm that backups were performed daily, including automated reporting on successful completion and storage at a remote SWIFT location.<br><br>• Inspect the restore test outcome to confirm that backups were restored on an annual basis for testing purpose.<br><br>Reperformed, for a sample of systems and databases, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **10.** | The business continuity plans and the ability to recover services and critical functions are tested on a regular basis. An annual Business continuity test plan is prepared and executed. Identified issues are logged, assessed and tracked for resolution. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the annual business continuity exercises to confirm that a business continuity test was executed to recover services and critical functions, and that identified issues were logged, assessed and tracked for resolution.<br><br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.2. Resilient architecture

Control objective: The messaging service infrastructure is designed to ensure the continuity of operations in line with documented service commitments.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Protection mechanisms against environmental hazards are in place in the SWIFT-owned Operating Centres (OPCs) and CCCs as well as leased standalone BAPs and CCCs. These protection mechanisms consist of:<br>• Fire detection and suppression systems;<br>• Water detection systems;<br>• Redundant air-conditioning systems; and<br>• Uninterruptible power supply (UPS) systems.<br>For SWIFT-owned OPCs and CCCs, the fire detection and UPS systems are inspected and tested at least once a year. Records of the testing and results are kept.<br>Protection mechanisms for leased standalone BAPs and CCCs are not under the direct control of SWIFT. SWIFT performs a yearly check with the vendor to make sure the protection mechanisms are tested at least annually. | Inquired with management to ascertain that the control operated as described.<br>Observed the SWIFT facilities to confirm that the facilities were equipped with the following protection mechanism:<br>• Fire detection and suppression systems;<br>• Water detection systems;<br>• Redundant air-conditioning systems; and<br>• Uninterruptible power supply (UPS) systems.<br>Inspected service records for the environmental hazard protection mechanisms at SWIFT facilities to confirm that the mechanisms were inspected and tested at least once a year.<br>Inspected vendor service documents to confirm that protection mechanisms at BAPs and CCCs not under direct control of SWIFT, were tested at least annually.<br>**No relevant exceptions noted** |
| **2.** | SWIFT messaging services reside in multiple operating centres. Each operating centre resides in a different country. SWIFT systems are deployed in such a way that each operating centre individually has the capacity to meet the processing requirements of the SWIFT user community in the concerned zone(s). | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the operating centres to confirm that SWIFT messaging services resided in multiple operating centres across different countries.<br>• Inspect that systems and networks essential to the main customer message processing were monitored on their usage and that trend analysis was performed based on the acquired data.<br>• Inspect a sample of months to confirm that capacity reviews were performed on the systems and networks essential to the main customer message processing and that upgrades were performed when needed following the capacity review.<br>• Inspect a sample of systems to confirm that system resources were being monitored on their Memory, Disk, |

| | | |
|---|---|---|
| | | Database and CPU usage and that alarms were generated when thresholds were exceeded.<br>• Inspect the annual test report to confirm that SWIFTNet and FIN redundancies achieved disaster site takeovers within 20 minutes for a single Zone Site Take-over, and within 30 minutes for a concurrent Site Take-over in two Zones.<br>**No relevant exceptions noted** |
| **3.** | The SIPN is designed to minimise the impact of any single component failure. Network Partners provide customer connectivity to multiple BAPs. The SWIFT backbone network is designed to provide resilient connectivity between the BAPs and the operating centres. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the infrastructure documentation of the BAP's and SBN, to confirm that:<br>– Critical components were resilient (no single component failure);<br>– The network partners provided connectivity to multiple BAPs;<br>– The connectivity from the BAPs to the SBN was setup in a resilient way; and<br>– SBN was designed to provide resilient connectivity between the BAPs and the OPCs.<br>**No relevant exceptions noted** |
| **4.** | All FIN customer traffic, SWIFTNet SnF traffic and SWIFTNet traffic flagged for the non-repudiation service is replicated between operating centres to meet data retention requirements. Replication may be deferred during disaster site takeover scenarios, Maintenance Windows and FIN SP switchover operations.<br>The status of message replication is monitored and alarms are generated when exceeding requirements. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect procedure for Production Operations to confirm that traffic replication monitoring was included in the defined process.<br>• Inspect configuration of monitoring of FIN customer traffic, SWIFTNet SnF traffic and SWIFTNet traffic flagged for the non-repudiation to confirm that replication monitoring was performed and in line with the data retention requirements.<br>• Inspect a sample of occurrence where message replication exceeded |

| | | |
|---|---|---|
| | | requirements to confirm that the problems were tracked until closure.<br><br>**No relevant exceptions noted** |
| **5.** | Customer messages that have a retention commitment (FIN messages, SWIFTNet SnF files and messages, and non-repudiation data) are stored redundantly at different operating centres. Handling and storage processes and procedures exist to help ensure that media storing this information is available for at least the committed period.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect handling and storage procedures to confirm that redundancy and committed period of availability were included in the defined process.<br><br>• Inspect configuration of monitoring of FIN customer traffic, SWIFTNet SnF traffic and SWIFTNet traffic flagged for the non-repudiation to confirm that a message flagged with a retention commitment was stored in at least two different operating centres.<br><br>• Inspect result of testing performed by management on non-production environment to confirm that management ascertained that a message flagged with a retention commitment was stored at least for the committed period.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.3. Availability monitoring

Control objective: Availability of the messaging services are monitored to detect and react to problems.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **1.** | System and network availability is monitored and reported against set targets. Instances of unavailability are logged in a tool and used to report availability results per the Service Availability Reporting Process. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of monthly production performance reports to confirm that system and network availability was monitored against set targets, and that instances of unavailability were logged and incorporated in the availability reports.<br>Reperformed, for a sample of monthly production performance reports, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **2.** | Multiple Central Control Centres (CCCs) monitor sequentially the messaging service infrastructure and SWIFT's operating centres 24 hours a day, 7 days a week. | Inquired with management to ascertain that the control operated as described.<br>Inspected staff schedules to confirm that multiple team members were scheduled to monitor sequentially the messaging service infrastructure and SWIFT's operating centres 24 hours a day, 7 days a week.<br>**No relevant exceptions noted** |
| **3.** | Responsibilities are formally assigned and documented to detect and react to operational problems.<br>All reported problems are logged in a trouble ticketing system, classified and tracked until closure. Timers and thresholds are formally defined to help ensure proper escalation of problems, up to activation of the Command Centre. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the operational procedures to confirm that responsibilities to detect and react to operational problems were formally assigned, timers and thresholds on escalation of problems were defined.<br>• Inspect a sample of problems to confirm that these were logged in a trouble ticketing system, classified and tracked until closure.<br>Reperformed, for a sample of problems, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate. |

| | | |
|---|---|---|
| | | Reperformed, for the operational procedures, SWIFT IA's tests over the procedures examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **4.** | Service availability results are included in the corporate key performance indicators that are used by management to assess the performance of the company. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of monthly corporate KPI scorecards to confirm that availability results were included and aligned with the monthly Production Performance Reports.<br><br>Reperformed, for a sample of monthly corporate KPI scorecards, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **5.** | The Operational Performance Report includes an overview of problems classified as incidents (as defined in Appendix A: Glossary) as well as performance against availability targets. This report is published to the Board on a quarterly basis and is reviewed during the Technology and Production Committee meetings. Any potential action is recorded in the TPC meeting minutes. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Operational Performance Report to confirm that this report included an overview of the problems classified as incidents as well as performance against availability targets, and this report was published to the board on a quarterly basis, and reviewed as well as actioned upon during the Technology and Production Committee.<br><br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.4. Business continuity and disaster recovery

Control objective: SWIFT has developed Business Continuity Plans and Disaster Recovery Plans in line with service commitments.

Note: Control 3.2.4.3 also applies to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| 1. | SWIFT has comprehensive policies and procedures as well as formally defined roles and responsibilities to ensure appropriate business continuity management and planning:<br>• Business impact analysis (BIA) is performed every year to validate the criticality classification of the services and business units including their recovery objectives.<br>• Business continuity plans (BCP) have been developed for each critical location/function and provide a plan (which includes amongst others recovery from cyber-attacks, data loss and pandemic diseases) to ensure staff safety/security and the recovery and continuity of critical business services within the agreed and pre-defined timescales (RTOs) in the event of an interruption.<br>SWIFT's business continuity framework is described in the Business Continuity Manual (BCM). The BCM and BCPs are reviewed annually and updated as necessary. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect SWIFT's Business Continuity Manual to confirm that roles and responsibilities were formally defined, and that the document was reviewed in the year and approved when updated.<br>• Inspect the Business impact analysis (BIA) to confirm that it was performed in the year and included the criticality classification of the services and business units including their recovery objectives.<br>• Inspect a sample critical location/function to confirm that a business continuity plan was developed, provided a plan to for staff safety/security and the recovery and continuity of critical business services within the agreed and pre-defined timescales (RTOs) in the event of an interruption, and was reviewed in the year and updated when necessary.<br>Reperformed, for a sample of critical location/functions, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, for the Business Continuity Manual and BIA, SWIFT IA's tests over the Business Continuity Manual and BIA examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.4 Business continuity and disaster recovery (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| **2.** | Annually, SWIFT facilitates the testing of user connectivity to the disaster recovery infrastructure and reconciliation of messages. A subset of customers are invited to participate in this testing. SWIFT uses defined criteria to select the critical customer locations. Identified issues are logged, assessed and tracked for resolution. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Simulation Support Master Plan to confirm that user connectivity and reconciliation of messages requirements were included in the plan.<br>• Inspect the annual test results to confirm that the test was performed in line with the requirements and that identified issues were logged, assessed and tracked for resolution.<br>**No relevant exceptions noted** |
| **3.** | The business continuity plans and the ability to recover services and critical functions are tested on a regular basis. An annual Business continuity test plan is prepared and executed. Identified issues are logged, assessed and tracked for resolution. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the annual business continuity test to confirm that the ability to recover services and critical functions was tested, and that identified issues were logged, assessed and tracked for resolution.<br>Reperformed, for the Business continuity test plan, SWIFT IA's tests over the test plan examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.5. Capacity management

Control objective: Processes and procedures are in place to ensure the messaging services infrastructure has sufficient capacity to process messages.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Systems capacity and network capacity, essential to the main customer message processing, are verified by usage monitoring, trend analysis of data and capacity reviews in order to perform any required upgrades. | Inquired with management to ascertain that the control operated as described.<br>Inspected monthly monitoring reports to confirm that systems and networks essential to the main customer message processing were monitored on their usage and that trend analysis was performed based on the acquired data.<br>Inspected a sample of months to confirm that capacity reviews were performed on the systems and networks essential to the main customer message processing and that upgrades were performed when indicated following the capacity review.<br>**No relevant exceptions noted** |
| **2.** | The use of system resources – for example, memory, disk and database space, and CPU utilisation – is monitored.<br>Alarms are generated if thresholds are exceeded and followed-up, if deemed necessary. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of systems to confirm that system resources were being monitored on their Memory, Disk, Database and CPU usage and that alarms were generated when thresholds were exceeded.<br>Inspected a sample of alarms to confirm that these were followed-up if deemed necessary.<br>**No relevant exceptions noted** |
| **3.** | Performance analysis is conducted for performance requirements recorded in functional requirement specifications and related documents. Benchmark testing is used to help ensure that the release meets the expected performance targets.<br>Major releases of FIN undergo benchmark testing. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of SWIFTNet and FIN releases to confirm the performance analysis was performed and that performance requirements were recorded.<br>Inspected a sample of major SWIFTNet and FIN releases to confirm that benchmark testing was performed in order to meet expected performance requirements.<br>**No relevant exceptions noted** |
| **4.** | SWIFT's Capacity Planning department has implemented a capacity planning process.<br>Capacity requirements have been defined to forecast the traffic, the capacity that is needed and how the supply will meet the required level of capacity per service. The plan is monitored against actual performance. In case of major | Inquired with management to ascertain that the control operated as described.<br>Inspected the capacity planning process document to confirm that a capacity planning process was defined and that requirements were defined to forecast traffic, the capacity that is |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | deviations, the Capacity Clearance Committee (CCC) decides on necessary actions. | needed and how the supply will meet the required level of capacity per service.<br><br>Inspected that capacity planning was monitored against actual performance.<br><br>Inspected for a sample of major deviations that the Capacity Clearance Committee decided on necessary actions.<br><br>**No relevant exceptions noted** |
| **5.** | The Capacity Clearing Committee (CCC) consists of the Group Heads – the CPO (also the Chair of CCC), the CIO and CFO representing Product, Technology Platform and Finance - together with the Head of Message Services, Platform Services, Strategic Architecture and Financial Planning & Analysis.<br><br>The roles and responsibilities of the CCC are defined in a charter. Their main role is to provide governance for the production capacity plan by validating, at the company level, traffic volume and peaks forecast for the different services, thus helping to ensure that adequate capacity is deployed at the right time.<br><br>The CCC meets at least once a year. The CCC evaluates the projected volumes by reviewing the capacity demand and the capacity supply. Based on this, the CCC assesses potential capacity risks and additional capacity deployment requirements. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the Capacity Clearing Committee charter to confirm that the roles and procedures were in line with the control description;<br><br>• Inspect the Capacity Clearing Committee meeting minutes to confirm that the traffic projections were discussed and decisions were timely communicated to relevant teams<br><br>Reperformed, for the Capacity Clearing Committee charter and meeting minutes, SWIFT IA's tests over the charter and meeting minutes examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |

# 3 Reliability and resilience

## 3.2.6. Message Validation

Control objective: SWIFT validates messages, and only validated messages are processed and delivered.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **SWIFTNet Specific** | |
| **1.** | The following validations must be successful for a SWIFTNet message to be delivered to the receiver for either real-time services or store-and-forward services:<br>• Presence and syntax of Requestor and Responder Distinguished Name (DN);<br>• The signing authority of the message must match that of its sender;<br>• The authenticating signature must be valid;<br>• Presence and validity of service name; and<br>• The requester is allowed to send messages to the responder as defined in the appropriate CUG.<br>Two optional validations may also be used with the following requirements:<br>• When the service requires RBAC, the existence of a role of the service granted to the Authoriser DN; and<br>• When the service uses MVAL, the document within the payload is validated against the appropriate schema.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the presence and syntax of Responder DN.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet validated that the signing authority of the message was the one of the sender DN.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the validity of the authenticating signature.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the presence and validity of service name.<br>• Inspect the results of management's test on non-production environment to confirm that the requester and the responder were allowed to communicate, i.e. were in the appropriate CUG.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed that the payload is valid against the MVAL schema for MVAL services.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed that the Authoriser DN was granted the role of the service.<br>• Inspect that management documented the basis for determining that non- |

| | | |
|---|---|---|
| | | production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **2.** | All successful customer-to-customer SWIFTNet responses are validated to check:<br>• Presence and syntax of Responder DN;<br>• The signing authority of the message must match that of its sender;<br>• The authenticating signature is valid;<br>• The responder matches the entity to which the original message was sent;<br>• When the service uses MVAL (which is optional), the document within the payload is validated against the appropriate schema; and<br>• For store-and-forward services, the Authoriser DN (Signer DN for MI Channel) in the store-and-forward acknowledgement must be the same as the Authoriser DN (Signer DN for MI Channel) that acquired the queue from which the message was delivered.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the presence and syntax of Responder DN for successful customer-to-customer responses.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet validated that the signing authority of the message was the one of the sender DN for successful customer-to-customer responses.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the validity of the authenticating signature for successful customer-to-customer responses.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed that the payload is valid against the MVAL schema for successful customer-to-customer MVAL responses.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet confirmed the matching between the Authoriser DN in the store-and-forward acknowledgement and the Authoriser DN that acquired the queue for successful customer-to-customer responses in the store-and-forward services.<br>• Inspect that management documented the basis for determining that non-production environment used for |

| | | |
|---|---|---|
| | | application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **3.** | If the customer uses SWIFTNet synchronous message transfer, the requestor's application is halted until it receives a response from the responder. When no response is received within a predefined period, SWIFT times out the requestor's SWIFTNet Link. The application receives notification if the request has timed out.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the requestor's application was halted until SWIFTNet received either a response either a time out notification in SWIFTNet synchronous message transfer mode.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a time-out period was defined in SWIFTNet.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **4.** | If the customer uses SWIFTNet asynchronous message transfer, the requestor's SWIFTNet Link keeps track of the responses, which have to be explicitly retrieved. A time-out period exists for waiting for a response. There are a maximum number of outstanding responses per process. The application can retrieve notification if the request timed out.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the requestor's SWIFTNet Link kept track of the responses in SWIFTNet asynchronous message transfer mode.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a time-out period of responses was defined in SWIFTNet.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the responses to message transfer could be retrieved in SWIFTNet asynchronous message transfer mode. |

| | | |
|---|---|---|
| | | • Inspect the results of management's test on non-production environment to confirm that management ascertained that a maximum number of outstanding responses was defined in SWIFTNet.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **5.** | If the optional store-and-forward mechanism is enabled for a business service, a SWIFTNet message can remain in a queue for a maximum of 14 days while it waits for delivery. After this period, SWIFT sends an abort notification to the sender of the message.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a time-out period of 14 days was defined for message in queue if the optional store-and-forward mechanism was enabled.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that no messages older than 14 days were in queue if the optional store-and-forward mechanism was enabled.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that if a message cannot be delivered within 14 days, the message was removed from the queue and an abort notification was issued if the optional store-and-forward mechanism was enabled.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **6.** | If a store-and-forward message is queued for delivery, SWIFT attempts message delivery to the customer. If a delivery acknowledgement is not received on an attempted message delivery, subsequent delivery attempts include information on the previous delivery attempt. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described. |

| | | |
|---|---|---|
| | The output sequence number can be used for detection of unauthorised message duplication, insertion or removal.<br><br>For services using MI Channel batching, the batch sequence number and range can also be used for detection of message duplication, insertion or removal.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | • Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFT attempted to deliver store-and-forward messages in queue.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that store-and-forward messages in queue contained information of any previous delivery attempt with sequence number.<br><br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **7.** | After a number of failed delivery attempts for a store-and-forward customer to customer message, SWIFT sends an abort notification to the sender.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inquired with management to ascertain that the control operated as described.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that SWIFT defined a threshold of failed delivery attempts to store-and-forward a customer to customer message.<br><br>Inspected the results of management's test on non-production environment to confirm that management ascertained that SWIFT informed the sender through an abort notification when the threshold was exceeded.<br><br>Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **8.** | If the customer is accessing MI Channel, the customer messages are sent to SWIFT as per SNL or MFP configuration. If no response is received from SWIFT within a predefined period, the customer's SNL or MFP session with MI Channel is aborted.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that messages from customer accessing Mi Channel were sent as per SNL or MFP configuration.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a time-out period was defined. |

| | | |
|---|---|---|
| | | Inspect the results of management's test on non-production environment to confirm that management ascertained that after the defined time-out period, the customer session with MI Channel was aborted.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **9.** | Processes are in place to validate all FIN input messages against SWIFT standards and syntax. Checks are performed on Session Numbers and Input and Output Sequence Numbers to detect any unauthorised duplication, insertion or interception of messages to or from a customer. Message syntax errors result in rejection of messages and the sender is notified. Any application layer protocol error results in an immediate abort of the current FIN or GPA application sessions.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FIN messages were validated against SWIFT standards and syntax.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFTNet validated that Sessions Numbers were unique and that Input/Output Sequence matched.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that duplicate message or message with incorrect sequence were not processed and notification was sent to the sender.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that application layer protocol error resulted in application session abortion.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **10.** | SWIFT validates messages, thus preventing Test and Training messages from being addressed to | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to: |

| | | |
|---|---|---|
| | live destinations, or live messages from being addressed to Test and Training destinations.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | • Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that Test and Training messages were not routed to live destinations.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that Test and Training destinations could not receive live messages.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **11.** | Only valid FIN messages are queued for delivery to the receiving customer. If a delivery acknowledgement is not received on an attempted message delivery, subsequent delivery attempts include a possible duplicate message (PDM) trailer with a reference to the previous delivery attempts.<br><br>It is the responsibility of the receiver to reconcile messages with PDM trailers to avoid duplicate message processing.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that an invalid FIN message was not queued for delivery.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that queues contained only valid FIN messages.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FIN messages in queue contained information of any previous delivery attempt with sequence number.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **12.** | A FIN message can remain in a queue for a maximum of 14 days while it waits for delivery. After this period SWIFT sends an abort notification to the sender of the message. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to: |

| | | |
|---|---|---|
| | Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | • Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that a time-out period of 14 days was defined for a FIN message in a queue.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that FIN messages older than 14 days were deleted from the queue.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that if a message cannot be delivered within 14 days, the message was removed from the queue and an abort notification was issued.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **13.** | A daily report of all undelivered FIN messages per sender is generated and delivered to assist the customer in identifying those messages that have not been delivered to the intended receiver.<br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that the generated daily report contained undelivered FIN messages.<br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that daily undelivered FIN messages report was configured to be generated on a daily basis.<br>• Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |
| **14.** | Processes are in place to validate that for all FIN input messages, via the Message User Group | Inquired with management to ascertain that the control operated as described. |

| | | |
|---|---|---|
| | mechanism, the sender and recipient are defined for the given FIN message type.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspect results of management's test on non-production environment to confirm that management ascertained that the definition of the sender and the recipient were defined for each FIN message type via the Message User Group mechanism.<br><br>Inspect results of management's test on non-production environment to confirm that management ascertained that without the definition of the sender and the recipient via the Message User Group mechanism, the FIN message was not processed.<br><br>Inspect that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **15.** | After a number of failed delivery attempts, SWIFT sends an abort notification to the sender of the message and does not make further attempts to deliver the message.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFT defined a threshold of failed delivery attempts.<br><br>• Inspected the results of management's test on non-production environment to confirm that management ascertained that SWIFT informed the sender through an abort notification when the threshold was exceeded.<br><br>• Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br><br>**No relevant exceptions noted** |
| **16.** | FIN generates a Non-Delivery Warning (MT 010) for urgent messages whose delivery acknowledgement is not received within 15 minutes.<br><br>Management tests this control at least once annually in a test environment that is functionally equivalent to SWIFT's production environment. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br><br>• Inquire with management to ascertain that the control operated as described.<br><br>• Inspect the results of management's test on non-production environment to confirm that management ascertained that SWIFT defined as 15 minutes the threshold of Non-Delivery Warning. |

| | |
|---|---|
| | • Inspected the results of management's test on non-production environment to confirm that management ascertained that FIN generated a MT 010 if no delivery acknowledgement received after the defined threshold.<br>• Inspected that management documented the basis for determining that non-production environment used for application functionalities testing was adequate.<br>**No relevant exceptions noted** |

# 4 Technology planning

## 4.1. Introduction

This section describes SWIFT's methods to plan for the entire lifecycle of the use of technologies and the selection of technological standards.

### 4.1.1. Technology vendor management

SWIFT has established agreements with the Network Partners and key technology suppliers to define the boundaries of responsibility, service level agreements (SLAs), and the processes to monitor compliance with the agreements and manage the relationship with key suppliers.

External connections for vendor support purposes are not available.

### 4.1.2. Technology Vendor Advisory Council

Given the predominant focus of SWIFT's technology and operational activities within Product and Technology Platform, SWIFT has set up an oversight body called the Technology Vendor Advisory Council (TVAC) to facilitate technology-related governance for the enterprise.

This Council serves as an enterprise-wide body to oversee technology decisions. The Council comprises the Chief Product Officer (CPO), designated senior managers reporting to the CPO and designated senior managers from other organisations within SWIFT. The Council specifies guidelines to cover various aspects of the technology lifecycle. This includes selection, acquisition, use, maintenance and the overall risk management across the whole cycle.

# 4 Technology planning

## 4.2. Control objective

The following control objective governs a series of applied controls relating to technology planning within SWIFT:

**1.** Vendor technology is evaluated before first use and during its lifecycle

The section hereafter describes the different controls in place to meet this objective.

### 4.2.1. Technology lifecycle

Control objective: Vendor technology is evaluated before first use and during its lifecycle

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | Through the National Member and User Groups Meetings SWIFT seeks feedback from its users for new or future products and services. Three weeks before the quarterly Board meetings, SWIFT shares the relevant board papers with the Chairpersons of the National Member Groups (NMGs) and User Groups (UGs). Prior to the board meeting, the Executive Committee reviews and takes the feedback into consideration for the Board. After the board meeting, a highlights report is shared with the community through the Chairpersons of NMGs and UGs summarising the relevant decisions taken per documented Board procedures. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of Board meetings to confirm that:<br>– relevant board papers were shared with the Chairpersons of the NMGs and UGs prior to the board meeting;<br>– prior to the board meeting, a review of customer feedback was performed by the Executive Committee or a member thereof; and<br>– after the board meeting, a highlights report was shared with the community through the Chairpersons of NMGs and UGs summarising the decisions taken during the meeting.<br>**No relevant exceptions noted** |
| **2.** | Technology Vendor Advisory Council (TVAC) helps align strategic IT use of vendor technology and ensures timely revision of the planned usage in view of the technology evolution.<br>TVAC meetings are scheduled on a monthly basis to assess technology used at SWIFT that may require replacement or to introduce new technology in the SWIFT environment. The evaluation consists of defining product and vendor selection criteria, evaluating against the criteria, and arriving at a recommendation.<br>TVAC annually determines "Strategic Technology" vendors and assigns owners who are responsible for the relationship management with the vendor. TVAC identifies "Strategic | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of monthly TVAC meeting minutes to confirm occurrence of the meetings and their attendance.<br>• Inspect a sample of IT projects to confirm that associated vendors were categorised for financial due diligence.<br>• Inspect the approved "Strategic Technology" vendors list to conform that |

| Control Applied | Work Performed / Observations |
|---|---|
| Technology" vendors that require additional senior management attention by considering critical projects, investment, or usage impact. | SWIFT relationship owner was assigned for each vendor.<br><br>Reperformed, for a sample of monthly TVAC meeting minutes and approved "Strategic Technology" vendors list, SWIFT IA's tests over the samples and list examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |

# 5 Communication with users

## 5.1. Introduction

This section describes how SWIFT provides users information to enable them to understand their roles and responsibilities in managing risks related to their use of the swift services in scope of this report.

### 5.1.1. SWIFT User Handbook

The customer environment can also affect the security of SWIFT services. SWIFT has identified specific roles and responsibilities applicable to customers, which are defined in the service descriptions and policies.

These documents are legally binding and usually published once a year and are collectively known as the *SWIFT User Handbook*. They form the contract between SWIFT and the customer.

### 5.1.2. Release management

The SWIFTNet Release Policy defines the principles for the release of SWIFTNet products and services. Timing and content of SWIFTNet releases are communicated to the customer through the Release Timeline and the SWIFT Operational Newsletter (if customer subscribes), published on SWIFT.com. SWIFTNet releases have been divided into the following categories:

- Major releases introduce major changes and enhancements that apply to all services and products within the scope of the SWIFTNet and Alliance release policy. Major releases apply to all customers. SWIFT announces major releases at least 18 months in advance of the date on which the release will go live in Production.
- Minor releases introduce either major changes and enhancements to a limited number of services and products, or minor changes and enhancements to several services and products and/or technology changes. Minor releases often apply to a limited number of customers only. SWIFT announces minor releases at least 9 months in advance of the date on which the release will go live in Production.
- Update releases introduce technology and/or security changes (such as hotfixes) or minor functional changes to a single product. Updates can apply to all customers or to a specific group of customers. SWIFT provides updates as required with prior notification.

When necessary, accelerated and emergency releases are deployed to fix serious problems.

### 5.1.3. Operational status updates

SWIFT uses SWIFT.com, among other channels, to inform customers of the status of the messaging service infrastructure. When a fault occurs, status updates are available to registered customers.

The online customer support service allows customers to search a knowledge base for known problems and workarounds. This information includes most frequently asked questions and answers, troubleshooting and diagnostic guidelines, and status reports about known problems. Furthermore, the customer may contact Global Support Delivery (GSD) to request assistance.

# 5 Communication with users

## 5.2. Control objectives

The following control objectives govern a series of applied controls relating to communication with users of the SWIFTNet and FIN services:

1. Roles and responsibilities between SWIFT and its customers are in line with documented service commitments;
2. Problems reported by customers are tracked, monitored and resolved in line with committed service levels;
3. Customers are provided product and service information to support them in understanding and managing their risks.

The sections hereafter describe the different controls in place to meet each of these objectives.

### 5.2.1. Roles and responsibilities

Control objective: Roles and responsibilities between SWIFT and its customers are in line with documented service commitments.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | It is a condition precedent of the use of SWIFT's messaging services that the customer has entered into all relevant contractual arrangements. These contractual arrangements and any subsequent amendments are maintained and securely stored. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of new customers to confirm that the customer entered into all relevant contractual arrangements with SWIFT precedent of the use of SWIFT's messaging services.<br>Inspected whether contractual arrangements and subsequent amendments were maintained and stored securely.<br>**No relevant exceptions noted** |
| **2.** | Service level agreements with customers are monitored and reported. Deviations are recorded and remedial actions are taken. | Inquired with management to ascertain that the control operated as described.<br>Inspected a sample of reports towards customers to confirm that service level agreements with customers were monitored and reported, and that in case of deviations, these were recorded and remedial action was taken.<br>**No relevant exceptions noted** |
| **3.** | The General Terms and Conditions and related service documentation formally define SWIFT's and customer's standard roles and responsibilities. If SWIFT updates the General Terms and Conditions, the updated draft is published on swift.com prior to coming into effect and lists key changes in the preface. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the General Terms and Conditions and related service documentation on swift.com to confirm that these defined SWIFT's and customer's standard roles and responsibilities. |

| | | |
|---|---|---|
| | | • Inspect SWIFT's newsletters to confirm that SWIFT employees, partners and customers were informed about updates to the General Terms and Conditions in a timely manner.<br><br>**No relevant exceptions noted** |
| **4.** | SWIFT assumes responsibility for the delivery of messages as defined in the service documentation. There is a formal process for the evaluation of customer claims whereby, if it is necessary to retrieve messages, the request must be initiated by the General Counsel and the Privacy Officer informed. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the procedure for handling customer claims to confirm that a formal process was in place for the evaluation of customer claims and that requests for message retrieval required initiation by the General Counsel and informing the Privacy Officer.<br>• Inspect the service documentation to confirm that SWIFT defined his responsibility for the delivery of messages.<br><br>**No relevant exceptions noted** |
| **5.** | The Service Description defines the features and functions of a product or service as well as the roles and responsibilities of SWIFT and customers in relation to that product or service. Procedures and guidelines for using the SWIFT products and services are provided in the corresponding User Documentation. The Service Descriptions and User Documentation are reviewed, updated and approved when there are changes to the product or service. The Service Descriptions and User Documentation are made available to registered customers on www.swift.com. An overview of all updated and new documents is available on the Knowledge Centre. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Service Description to confirm that features and functions of a product or service as well as the roles and responsibilities of SWIFT and customers in relation to that product or service were defined.<br>• Inspect a sample changes to product or services to confirm that Service Descriptions and User Documentation were reviewed and approved.<br>• Inspect www.swift.com to confirm that Service Descriptions and User Documentation were available to registered customers.<br>• Inspect the Knowledge Centre to confirm that updated and new documents were available.<br><br>**No relevant exceptions noted** |

# 5 Communication with users

## 5.2.2. Problem and status reporting

Control objective: Problems reported by customers are tracked, monitored and resolved in line with committed service levels.

Note: Controls 5.2.2.2 and 5.2.2.4 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | To allow customers to submit questions, report problems or inquire on the status of previously reported problems, SWIFT provides customer helpdesk services 24 hours a day, 7 days a week.<br><br>Global Support Delivery (GSD) acts as the single point of contact for customers who have issues with SWIFT products or services or SWIFT connectivity. GSD is located on different continents and observes a follow-the-sun approach. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Process Management Framework and procedures to confirm that SWIFT provides customer helpdesk services 24 hours a day, 7 days a week.<br>• Inspect a sample of days to confirm that GSD acted as the single point of contact for customers having issues with SWIFT product, services or connectivity, and that the follow-the-sun approach was implemented.<br><br>Reperformed, for a sample of days, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>Reperformed, for the Process Management Framework and procedures, SWIFT IA's tests over the Process Management Framework and procedures examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **2.** | SWIFT has processes in place to provide operational status updates to registered customers for service interruptions and incidents. These processes document which communication channel(s) will be used to inform customers. If a service incident occurs, SWIFT makes an incident report available to the | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Incident Manual and Crisis Manual to confirm that SWIFT had |

| | | |
|---|---|---|
| | customers within five business days of the time of the event. | documented procedures for providing operational status updates on service interruptions and incidents to registered customers.<br>• Inspect a sample of incidents to confirm that an incident report was made available to customers on a timely basis.<br>Reperformed, for a sample of incidents, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>Reperformed, for the Incident Manual and Crisis Manual, SWIFT IA's tests over the manuals examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **3.** | All customer requests for assistance are logged and tracked until successfully closed using a support ticketing system. For every case created the customer is given a unique case number, which serves as a unique reference to the problem or query. Customers who are properly registered can access online support and can access their own cases as well as cases created on their behalf. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of customer requests to confirm that the requests were logged and tracked until successfully closed in a trouble ticketing system and a unique case number was assigned.<br>• Inspect the system configuration to confirm that only registered customers were able to access their own cases as well as cases that were created on their behalf.<br>Reperformed, for a sample of customer requests, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br>**No relevant exceptions noted** |
| **4.** | SWIFT has documented procedures in place to handle crises/incidents that have a severe impact on SWIFT (reputation, media attention, financial or legal exposure) or its community. The Crisis Manual defines formal roles and responsibilities and describes the steps to be taken in case of a crisis or major incident. The Crisis Manual is reviewed and updated at least annually to incorporate lessons learned from crisis and major incidents. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Crisis manual to confirm that formal roles and responsibilities were defined as well as the steps to be taken care in case of a crisis or a major incident, and that the Crisis Manual was reviewed and updated at least yearly.<br>Reperformed, for the Crisis manual, SWIFT IA's tests over the manual examined to ascertain |

| | | |
|---|---|---|
| | | whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| | **FIN Specific** | |
| **5.** | SWIFT has processes and procedures to ensure that SWIFT responds to requests from national representatives for urgent broadcasts, for example for a national strike or political unrest, within two hours. If SWIFT is unable to process the request within this time, SWIFT will notify the requester within two hours. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the broadcast process to confirm that SWIFT had processes and procedures to respond to requests from national representatives for urgent broadcasts within two hours.<br>• Inspect for a sample of requests from national representatives to confirm that SWIFT responded either within two hours or notified the requester within two hours that SWIFT was unable to process within the timeframe.<br>Reperformed, for a sample of requests from national representatives, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **6.** | SWIFT has processes and procedures to ensure that SWIFT sends a broadcast notifying users within five business hours when receiving a notification of closure, for example for an extended holiday or individual bank strikes. If it is not possible to send the broadcast within five hours, the representative requesting the broadcast will be notified within that period. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the broadcast process to confirm that SWIFT had processes and procedures in place to notify users within five hours when receiving a notification of closure.<br>• Inspect a sample of notifications of closure to confirm that SWIFT either notified users within five business hours or notified the requestor that it was not possible to send the broadcast within the agreed timeframe.<br>Reperformed, for a sample of notifications of closure, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |

# 5 Communication with users

## 5.2.3. Risk reporting

Control objective: Customers are provided product and service information to support them in understanding and managing their risks

Note: Controls 5.2.3.5 also apply to the following SWIFT.com services:

- e-Ordering;
- Online Customer Support;
- Secure Channel;
- Download Centre;
- Operational Status communication; and
- Communication of the Release Timeline.

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | **Core** | |
| **1.** | SWIFT makes the On-line Knowledge Base, Documentation and Download Centre available on www.swift.com to registered users. SWIFT provides information about known issues or warnings identified on a given software version. Software issues raised by customers are tracked. Confirmed issues, potentially impacting other customers, are documented in articles and published on-line providing a description of the problem, the symptom(s) and the workaround (if any).<br><br>A list of resolved problems is provided at the time a new software version is made available and related articles are updated to indicate the problems that are fixed in the newly released version. Significant software issues (or warnings) are also listed in an article linked to the software version (Known Issues and Warnings). | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect www.swift.com to confirm that:<br>– information was provided about known issues or warnings identified on a given software version; and<br>– confirmed issues (or warnings) were documented in articles and published on-line providing a description of the problem, the symptom(s) and the workaround (if any).<br>• Inspect a sample of software issues raised by customers to confirm that a ticket was recorded.<br>• Inspect a sample of releases to confirm that a list of resolved problems at the time of the new release was made available and related articles were updated.<br><br>Reperformed, for a respective samples of software issues, releases and publications on SWIFT.com, SWIFT IA's tests over the samples examined to ascertain whether the conclusions reached by SWIFT IA were appropriate.<br><br>**No relevant exceptions noted** |
| **2.** | Mass roll-out activities requiring customer action are organised through campaigns by Contact Data and Campaign Management. Campaigns | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to: |

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | are required for all major and mandatory roll-outs. Each campaign has a dedicated campaign manager and plan which defines campaign objectives, key milestones, deadlines and the communication activities to be executed. | • Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample of major and mandatory roll-out activities to confirm that a dedicated campaign manager was assigned and a campaign plan was created defining the campaign objectives key milestones, deadlines and the communication activities to be executed.<br>**No relevant exceptions noted** |
| **3.** | The SWIFT Corporate Rules define the SWIFT User categories and specify the eligibility criteria and the admission and termination rules applicable to SWIFT users.<br>The SWIFT By-laws define the purpose of the company and specify the fundamental rules on the admission of shareholders, shareholding, the election and functioning of the Board of Directors, and holding of General Meetings. The SWIFT General Terms and Conditions govern the provision and use of the SWIFT services and products in scope.<br>These documents are publicly available on swift.com. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the SWIFT Corporate Rules to confirm that SWIFT User categories were defined as well as the eligibility criteria and the admission and termination rules applicable to SWIFT users were specified.<br>• Inspect the SWIFT By-laws document to confirm that the purpose of the company was defined as well as the fundamental rules on the admission of shareholders, shareholding, the election and functioning of the Board of Directors, and holding of General Meetings were specified.<br>• Inspect SWIFT General Terms and Conditions to confirm that these governed the provision and use of the SWIFT services and products in scope.<br>• Inspect the swift.com portal to confirm that the documents were publicly available on this website.<br>**No relevant exceptions noted** |
| **4.** | All planned major releases (related to SWIFTNet, FIN, Standard) must be published at least 18 months in advance and in case of minor releases at least 9 months in advance of the date on which the release will go live in Production. Updates are announced as necessary. End of support releases are 36 months from the time of the last major release.<br>The Release Timeline is updated approximately every 3 months and published on | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect a sample major and minor releases of SWIFT-DiCoA interface/leg to confirm that these were published sufficiently in advance of the go live date, and that the release timeline was |

# 5 Communication with users

## 5.2.3 Risk reporting (continued)

| | Control Applied | Work Performed / Observations |
|---|---|---|
| | www.swift.com. Customers can register to the SWIFT Notification Centre on www.swift.com to receive ad-hoc information. | regularly updated and published on www.swift.com.<br>• Inspect www.swift.com to confirm that customers could register to the SWIFT Notification Centre to receive ad-hoc information.<br>**No relevant exceptions noted** |
| **5.** | SWIFT plans and notifies customers in advance on www.swift.com of specific dates on which, and times at which, the service is unavailable.<br>Planned unavailability can be for the following events:<br>• Downtime due to scheduled equipment maintenance<br>• Scheduled system changes (for example, changes to software or hardware configurations or business continuity testing). | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect www.swift.com and planned maintenance schedules to confirm that customers were notified in advance of specific dates on which, and times at which, the service was unavailable.<br>**No relevant exceptions noted** |
| | **SWIFTNet Specific** | |
| **6.** | The Resilience Guide provides an institution with practical recommendations for building an appropriate level of resilience (that is, availability and reliability) into its global SWIFTNet messaging operations. It addresses the following aspects of resilience:<br>• Recommended resilience options<br>• SWIFTNet access resilience<br>• HSM resilience<br>• Resilience of messaging applications that link directly to SNL<br>• Resilience and performance of messaging applications using a communication interface<br>The Resilience Guide is reviewed and updated with each major release or significant change of a product or service. New versions are made available to the customers on www.swift.com where customers have the option to subscribe to automatic notification service in which case the customer receives a notification as soon as an update to a guide has been published. | Inspected SWIFT IA's documentation of the tests for the control to confirm that IA performed procedures to:<br>• Inquire with management to ascertain that the control operated as described.<br>• Inspect the Resilience Guide to confirm that recommendations for building an appropriate level of resilience were provided and included the aspects listed per the control.<br>• Inspect a sample of major releases to confirm that the Resilience Guide was reviewed, updated and made available on www.swift.com.<br>**No relevant exceptions noted** |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Activation secrets | A pair of passwords that either the customers' certificate administrator or the SWIFTNet Registration Authority (RA) issues to a subscriber when the subscriber has successfully registered to a service. The subscriber uses these secrets only once during the activation process, after which the secrets become invalid. |
| Agile Control Framework | The Agile Control Framework, is a set of activities that must be performed to support business objectives and covering the full Product Delivery lifecycle (amongst others development, testing and deployment). |
| Alliance Access Integration Platform (IPLA) | A licence option for Alliance Access that extends Alliance Access with integration functionality between users' backoffice systems and SWIFT. |
| Application Closed User Group (Appl-CUG) | Closed User Group application level. This is the list of allowed source and destination BIC combinations used to validate what client BICs can be used to access a service provider's web server as part of a SWIFTNet service using Browse. |
| Application Programming Interface (API) | A set of formalised software calls and routines that other applications can reference. Programmes reference an application's API to invoke the functionality of that application. |
| Audit and Finance Committee (AFC) | The SWIFT governance and oversight body for systems security, internal control, and financial policy. The full SWIFT Board approves the AFC's charter of activities. |
| Australia New Payments Platform (AU-NPP) | Payments market infrastructure for real-time payments in Australia. |
| Backbone Access Point (BAP) | A physical site that SWIFT manages and controls, from which the partner networks connect to the SWIFT Secure IP Network (SIPN). |
| Bank Identifier Code (BIC) | A code used in automated processing. This code unambiguously identifies a financial institution, or an entity within a financial institution. The ISO 9362 standard specifies the elements and the structure of a BIC. A BIC consists of either eight (BIC8) or 11 (BIC11) contiguous characters. These characters comprise either the first three, or all four, of the following components: bank code, country code, location code, and branch code. |
| BIC Directory | The SWIFT directory that lists the bank identifier codes (BIC) that SWIFT has registered according to the ISO 9362 standard, and the names and addresses of the corresponding entities. It also contains additional information, for example, the market infrastructures in which the entities participate. The scope of the additional information varies according to the version of the directory. Since January 2007, the BIC Directory is updated on a monthly basis and available for download on SWIFT.com. |
| Browse | A SWIFTNet messaging service that enables a secure, browser-based access, from an operator using a standard browser, to a service provider's web server. The original Browse implementation only supports access from Alliance WebStation or WebPlatform, over the Secure IP network (SIPN). The offering has been extended to also support Non-Repudiation and direct browser access over the Internet. |
| Business Continuity Planning (BCP) | A management process that provides a framework to build SWIFT resilience. This process also provides the capability for an effective response that safeguards the interests of SWIFT's stakeholders, reputation, and value-creating activities. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Central Control Centre (CCC) | A Central Control Centre (CCC) is an area formally dedicated to the monitoring and managing of SWIFT's network, production and internal systems. |
| Central institution | An organisation that performs a clearing, netting, or settlement function for a financial community, within a SWIFTNet or FINCopy service. A central institution is typically, but not necessarily, a national or central bank. |
| Certificate | A digital certificate, used for messaging services, is an electronic file signed by the Certification Authority (CA) that contains the end user's public key and that identifies the owner. |
| Certification Authority (CA) | A central system at SWIFT for producing and publishing digital certificates. |
| Checksum trailer (CHK) | A trailer that appears on all General Purpose Applications (GPA) and FIN messages. The CHK trailer enables the recipient to verify that the message has not been corrupted during transmission. |
| Chief Risk Officer (CRO) | Owns the Enterprise Risk Management (ERM) framework and facilitates risk assessments relating to relevant operational, strategic, reputational and financial risks per that framework. |
| Closed User Group (CUG) | A subset of customers that SWIFT has grouped to use certain SWIFT services and products when those customers access a specific, value-added business service. Either SWIFT or a service provider can provide this service. Sometimes also referred to as CGU. |
| Commercial off-the-shelf (COTS) | Non-SWIFT software purchased from an external supplier. |
| Continuous Linked Settlement (CLS) | The Continuous Linked Settlement (CLS) system is a special-purpose utility for settling high-value payments associated with foreign exchange (FX) transactions. The defining purpose behind the creation and implementation of CLS was to reduce systemic settlement risk in the world's FX market. |
| CPU | Central Processing Unit. |
| Customer Security Management (CSM) | The SWIFT department that administers security for SWIFT users. CSM also assists the SWIFT trusted third-party organisation (internal audit) with delivery investigations, claims, and authorisations for straight-through processing. It acts as the SWIFTNet Registration Authority (RA) for SWIFTNet security officers, and the Entrust administrator for SWIFTNet public key infrastructure (PKI). CSM also issues SWIFTNet Link Tuxedo passwords and acts as the SWIFTNet Certification Authority (CA) for SWIFT users' public RSA keys. |
| Customer Security Programme (CSP) | The programme that SWIFT has set up to help the SWIFT user community improve cybersecurity and to facilitate cybersecurity risk assessment by and amongst users directly. |
| Customer Operations | The SWIFT department that, among other duties, administers all customer registration details, creates and maintains the SWIFT database, and collects data for the BIC Directory. |
| Cyber defence | SWIFT's cyber defence is a subset of SWIFT's information security controls. SWIFT's cyber defence encompasses logical access related as well as other controls that aim to prevent a malicious act from taking place. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Cyber Fusion Centre | Team in Global Security designed to ensure global awareness, detection and response to cyber incidents. |
| Distinguished Name (DN) | The identification of an entity following the X.500 notation. SWIFTNet identifiers have the format of a DN. An example is *cn=xyz, ou=abc, o=bankbebb, o=swift*, in which *bankbebb* is the 8-character BIC, and the other elements at the left form the optional extension. This extension enables detailed identification by department, geographical location, application, or individual. |
| Domestic Messaging Channel (DMC) | A component of the Distributed Switch responsible for performing the reliable messaging for AU-NPP. It is part of the SWIFT interface and provides the reliable messaging and security capabilities for communication with other Participants. |
| End-to-end Common Overview Method for services and Products At SWIFT (ENCOMPASS) | The SWIFT methodology that improves the development and delivery of services and products for both internal and external customers. |
| Enterprise Risk Management (ERM) | Management of risks at the organisational level as it relates to the implemented risk management framework. |
| Extensible Mark-up Language (XML) | A standard for data representation and manipulation. XML is a meta-language that has been specifically designed for describing and exchanging structured data on the World Wide Web. |
| FileAct | An automated SWIFTNet messaging service that SWIFT has designed to enable customers to exchange files. FileAct supports both interactive and Store-and-Forward modes. It is particularly suited for the exchange of large volumes of data. |
| FIN | A SWIFTNet messaging service that allows the secure and reliable exchange of SWIFT MT standards in Store-and-Forward mode. User-to-user, user-to-SWIFT, and SWIFT-to-user messages are sent and received within the FIN service, that is, within both the General Purpose Application (GPA) and the financial messaging (FIN) application. |
| FINCopy Service | The SWIFT service in which the FINCopy service administrator or another destination, designated by the service administrator, fully or partially copies and optionally authorises, specific FIN messages that users exchange within a FINCopy closed user group. |
| FINInform | FINInform is an optional message copy service for message monitoring, reporting and optionally authorisation. The FINInform service copies all or part of a message to one or more copy destinations. The FINInform service works on the basis of a closed user group. |
| Federal Information Processing Standards (FIPS) | A set of standards developed by the National Institute of Standards and Technology for use by the U.S. government. FIPS use algorithms and cryptographic functions to ensure security. FIPS 140-2 is one of the more commonly known FIPS standards that specifies security requirements related to the design and implementation of cryptographic modules. |
| Four eyes principle | The principle that requires two individuals to carry out a sensitive task. |
| Front-End Processor (FEP) | A processor at a SWIFT Operating Centre (OPC) or a user site. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| General Purpose Application (GPA) | The SWIFT application that establishes and controls the communication between a Logical Terminal (LT) and the FIN service. The GPA also controls the user's initiation and termination of FIN sessions. |
| Global Security (GS) | The department within IT that is responsible for risk analysis, defining and maintaining corporate security and cyber defence policies and evaluation of cryptographic security implementation, as well as architecture design and requirements engineering. |
| Global Support Delivery (GSD) | The first-level helpdesk facility for customer queries and problems. |
| Global Zone | A global zone is a messaging service which is not restricted to customers in a particular region or country. SWIFT currently has two global zones, the EU and the TA zones. A global zone groups a set of countries, defined by the country code in the master BIC. All BICs of a country belong to the same zone.<br>Since the scope of this document does not cover local zone services, the term 'zone' in this document means 'global zone' unless it is prefixed by the word 'local'. |
| Hardware Secure Module (HSM) | Hardware Security Module (HSM) is a physical device used for securely generating and storing cryptographic keys and performing cryptographic operations such as digital signing. There are two types of HSMs offered to SWIFT customers:<br>• Local Area Network (LAN)-based HSM for managing low-to-high traffic volumes. The LAN-based HSM boxes follow FIPS 140-2 level-3 security standard and have active tamper detection and response mechanisms to prevent key compromise.<br>• Universal Serial Bus (USB)-based HSM for managing low traffic volumes: USB-based HSMs follow FIPS 140-2 level-2 security standard and offer mechanisms to provide evidence of any attempt at tampering with the system. |
| Human Intrusion Testing (HIT) Exercise | Human Intrusion Testing (or HIT Exercises) are cyber and social-engineering exercises conducted to test our physical and logical security. |
| Hypertext Transfer Protocol (HTTP) | The protocol used to transfer data across an Internet Protocol connection. |
| Hypertext Transfer Protocol Secure (HTTPS) | The protocol used to transfer data securely across an Internet Protocol connection. |
| Incident | Based on the following definitions, availability problems are categorised as a Service incident or Customer incident:<br>• Service incidents: SWIFTNet or FIN service problems where the service is unavailable or degraded, outside of allowable downtime windows, to one or more large customers or market infrastructures, during their business hours, and/or to more than 50 customers, for more than ten minutes, and where the SWIFT services, applications or networks are a cause of the problem.<br>• Customer incidents: When customers with a formally identified critical customer location are isolated for more than 30 minutes, if the problem occurs during their business hours and if SWIFT is the potential cause of the isolation. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Information security | Information security is the body of technologies, processes and practices designed to protect networks, computers, programs, services, data, associated premises and people from internal or external threats, including cyber-attacks. |
| Integration Testbed (ITB) | A network domain that vendors and developers use to test applications or interfaces before deployment on SWIFT's production network. |
| InterAct | A SWIFTNet messaging service that allows the interactive (real-time) and Store-and-Forward exchange of messages between parties. This service is particularly suited for mission-critical and time-critical applications. |
| Internet Protocol – Secure (IP-Sec) | An industry standard technology that SWIFT uses to secure all IP-based communication flows between the customer premises and SWIFT. |
| Internet Protocol (IP) | The accepted standard networking protocol for computer-to-computer communication. |
| IP Closed User Group (IP CUG) | Closed User Group at IP level. This is the list of allowed source and destination IP address combinations used to validate what computers can be used to access a service provider's web server as part of a SWIFTNet service using Browse. |
| ISO 27002 | International Organisation for Standardisation guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation. |
| Local zone | A local zone is a messaging service which is only available to customers in a particular region or country. |
| Local zone infrastructure | A local zone infrastructure consists of the hardware and software that support a local zone. |
| Maintenance Window (MW) | A scheduled period during which SWIFT does not guarantee service availability. Generally SWIFT uses MWs for planned changes that may interrupt services. |
| Major Release | Major releases introduce major changes and enhancements that apply to all services and products within the scope of the SWIFTNet and Alliance Release Policy. Major releases apply to all customers. |
| Managed Customer Premises Equipment (MCPE) | The network equipment that is located at the customer's site, and managed by SWIFT and its Network Partners. The MCPE consists of one or more VPN boxes and one or more network routers. |
| Market infrastructure (MI) | A system that provides services to the financial industry for trading, clearing and settlement, matching of financial transactions, and depository functions. Administrators of market infrastructures can be public organisations (for example, central banks) or other public instrumentalities, or private and regulated associations or entities. A market infrastructure encompasses a set of business rules and obligations, admission rules, operating rules, business communication flows, and related communication channels. |
| Market Infrastructure Resiliency Service (MIRS) | A generic payment settlement system operated by SWIFT on behalf of a market infrastructure in the event that the market infrastructure's Real Time Gross Settlement (RTGS) system is completely unavailable. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Message Reception Registry (MRR) | The registry where SWIFT stores the central routing rules. Each receiver defines its own rules and provides them to SWIFT. SWIFT uses these routing rules to determine where to deliver traffic, that is, to which Store-and-Forward queue or to which SWIFTNet Link (SNL). |
| Message User Group (MUG) | A group that FIN users need to belong to if they want to receive a particular category of standard messages, or specific Message Types. Users not registered for a particular MUG cannot send or receive the messages specified for use in that MUG. |
| Message usage restrictions | Limitations to the use of SWIFT messaging services in accordance with the respective user's eligibility criteria. |
| Messaging service infrastructure | This consists of all the components required for the live delivery of SWIFT's messaging services. These include SWIFTNet and FIN systems, SIPN, SNL, security management processes and underlying operational processes such as provisioning, operations, support and problem management, deployment and change management. Test environments or services, such as SWIFTNet's integration testbed, are not covered. |
| MI Channel | MI Channel (Market Infrastructure Channel) is a messaging channel that is designed to enable customers to access large market infrastructures in an efficient manner. It relies on the SWIFTNet Store-and-Forward platform, and optimises the exchange of large amounts of data between the market infrastructure and their participants, while offering a simplified mode of operation and facilitating integration. |
| Minimal Foot Print (MFP) | Alternative to SNL offered to a few Market Infrastructures, whose requirements cannot be addressed by the standard SNL software. |
| Minor Release | Minor releases introduce either major changes and enhancements to a limited number of services and products, or minor changes, enhancements, and/or security updates to several services and products and/or technology changes. Minor releases often apply to all customers or to a specific group of customers. |
| National Member Groups (NMGs) | A group that consists of all SWIFT Shareholders (members) within the same nation. The National Member Group advises and assists the Board of Directors on specific local matters. |
| Negative user acknowledgement | The rejection of a message input to a SWIFTNet messaging service. An error code indicates the reason for the rejection. |
| Network Device | Network devices consist of network connected routers, switches, firewalls and VPN concentrators. |
| Network Management System (NMS) | A comprehensive system of equipment used to monitor, control, and manage a data communications network. |
| Network Partner | An independent network provider selected by SWIFT to provide an IP Virtual Private Network (VPN) service offering to SWIFT customers, in respect of technical and performance requirements agreed with SWIFT. |
| Non-repudiation | The fact that an action cannot be denied after a given event. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Non-Repudiation Service (NRS) | An optional feature of InterAct, FileAct and Browse designed to provide access to data that can be used to obtain certainty with regard to the authenticity of the origin, the emission of the message (or file, in the case of FileAct), and optionally the reception of the message (or file, in the case of FileAct). |
| Normal operating conditions | Operations not hindered by an incident, in crisis or in BCP modus. |
| Operating Centre (OPC) | The site from which SWIFT operates and controls its systems. SWIFT has several Operating Centres throughout the world. |
| ORT | Operational Readiness Testing is the final set of tests to help ensure SWIFT is operationally ready for new services. |
| Payment Gateway (PAG) | It is a software component part of the SWIFT interface that embeds the business logic for the various messaging flows and provides the interface to the back-office application for AU-NPP. It communicates with other Participants through the Domestic Messaging Channel (DMC) software and with the back-office application through IBM MQ. |
| Payload | The part of an InterAct request or response that contains the business content of the request or response. |
| Point of Presence (POP) | The access point used to interconnect users and the Network Partner's network. |
| Possible Duplicate Message (PDM) trailer | A trailer added to a FIN message by the FIN system. The PDM trailer aims to warn the receiver that the same message may already have been output by FIN. The receiver may therefore receive the message twice, and must reconcile received traffic to avoid duplicate processing. |
| Post Incident Management Review (PIMR) | A process to outline the cause and planned actions to prevent recurrence of significant incidents. |
| Public Key Infrastructure (PKI) | A security infrastructure based on public key cryptography that provides digital signatures and the supporting certification services. SWIFTNet PKI comprises the SWIFTNet Certification Authority (CA), the SWIFTNet Registration Authority (RA), and the SWIFTNet Directory (SND). These authorities provide the customer with online certificate management capabilities. |
| RAID | Redundant Array of Independent Disks. |
| Real Time Gross Settlement (RTGS) | The settlement of payments in real time, and on a gross basis, across accounts held at a central bank. |
| Relationship Management Application (RMA) | The generic correspondent control mechanism that allows users to control what they want to receive from whom in a given service. |
| Release | Releases (or mark release) introduce major changes and enhancements that are relevant for a large set of customers. The installation and use of the SWIFTNet integration software products associated with a mark release is at the customer's discretion until it becomes mandatory six months after the mark release becomes generally available or such later date as communicated by SWIFT. SWIFT typically issues mark releases every 12 to 18 months. Major releases of FIN are interchangeably called Mark or Major releases. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Role-Based Access Control (RBAC) | An optional SWIFTNet facility that enables to control access to service functions by end users and applications. The service administrator defines the available user access profiles (roles) for use with RBAC. After provisioning, the Security Officers (SO) within an institution can grant roles to end users and applications. |
| Secure IP Network (SIPN) | SWIFT's worldwide, highly secure, and extremely reliable Virtual Private Network (VPN). The SIPN is based on the Internet Protocol and related technologies and provides transport services required by SWIFTNet services. |
| Secure Login and Select (SLS) | A SWIFT service used to log on to the General Purpose Application (GPA) and to select the FIN service using PKI digital signatures performed on Hardware Security Modules. |
| Security and Reliability Committee (SRC) | The SRC is in place to help ensure consistency in oversight over the definition, implementation and improvement of the security control framework. This framework consists of policies, standards and processes that are used to manage risk to SWIFT's commitments regarding confidentiality, integrity and availability. |
| Security Council (SC) | The SC is in place to provide the CEO with oversight of security-related decisions and impacts. Security is defined as comprising confidentiality, integrity and availability. |
| Security Incident | An incident that does not impact the availability of SWIFT's main messaging services, but impacts the confidentiality or integrity of the main message flow. Security incidents may be the result of malicious acts, like cyber-attacks, or unintentional events, like software failures (bugs) (see also definition of incident). |
| Service Administration Request Form (SARF) | Form used by service administrators to add or delete members from the relevant CUG or MUG. |
| Service Bureau | A non-SWIFT user organisation that provides users with services regarding the day-to-day operation of their SWIFT connection, such as hosting or operating SWIFT connectivity components, logging in, or managing sessions or security for SWIFT users. To avoid any doubt, an organisation that only installs or maintains interfaces must not register as a Service Bureau. |
| Service Level Agreement (SLA) | A contractual obligation for a service provider to meet a particular level of quality of service. SLAs can apply on service availability, performance and throughput, as well as on the support services. |
| Service Partner | An independent company that has agreed with SWIFT to offer SWIFT customers specific services, such as implementation services, in connection with the provision of SWIFT service and products, and in accordance with predefined quality standards. |
| Slice Processor (SP) | The processor within FIN that performs the routing and safestore of messages. Each SP owns (that is, is in control of) a number of specific destinations. |
| Standards | The overarching name for standards products, tools, and services that SWIFT delivers to the SWIFT community. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| Store-and-Forward (SnF) | A communication or messaging methodology that SWIFT has designed to enable users/subscribers to exchange messages by means of a central storage facility. The correspondents must not be simultaneously connected to the central storage facility. Communication between correspondents is indirect and comprised of two independent direct communications: sender to central storage facility, and central storage facility to receiver. Examples include the FIN messaging service, other SWIFTNet messaging services in Store-and-Forward mode, and Mail services. |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication, Societé Coopérative. SWIFT is a trademark and the trading name of S.W.I.F.T. SC. SWIFT is the industry-owned co-operative (limited co-operative society) which supplies secure messaging services and interface software to a large community of financial institutions. |
| SWIFT By-Laws | The SWIFT By-laws define the object to the company and set out the rules about *inter alia* the admission of shareholders, shareholding, election and functioning of the Board of Directors, and the holding of the General Meeting. |
| SWIFT Corporate Information Security Policy (SCISP) | The set of policies that define policies adhered to by all of SWIFT. |
| SWIFT user | An organisation admitted to the SWIFT messaging services as described in SWIFT SC's Corporate Rules and By-Laws. |
| SWIFT User Handbook (UHB) | The set of documents, amended from time to time, that constitutes a contractual basis for the operational relationship between SWIFT and any SWIFT user. |
| SWIFT's Applications | A SWIFT portfolio of sophisticated, standardised and automated solutions that members can use to interoperate with their counterparties in payments, trade, treasury, and securities. |
| SWIFTNet | The SWIFT advanced IP-based messaging platform. It comprises a portfolio of services and products that enable customers to communicate mission-critical financial information and transactional data securely and reliably. |
| SWIFTNet Directory | An online repository of institutions connected to SWIFTNet, and the PKI certificates and role-based access control (RBAC) roles issued to the operators, applications and interfaces of these institutions. |
| SWIFTNet Interface | A computer system operated by a SWIFT user to communicate with the SWIFT advanced IP-based messaging platform. |
| SWIFTNet Link (SNL) | The mandatory software product required before a customer can access SWIFTNet messaging services over the Secure IP Network (SIPN). |
| SWIFTNet messaging services | These are the messaging services available on the SWIFT Secure IP Network (SIPN). The SWIFTNet messaging services include FIN, InterAct, FileAct, and Browse. |
| SWIFTNet PKI | A pervasive security infrastructure based on public-key cryptography, which provides digital signatures and supporting certification services. SWIFTNet PKI comprises the SWIFTNet certification authority, the SWIFTNet registration authority, and the SWIFTNet directory, which provide the customer with online certificate management capabilities. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| SWIFTNet Registration Authority (RA) | A SWIFT-registered body that is responsible for identifying and authenticating an institution and the initial users of the SWIFT public key infrastructure (PKI) (for example, an institution's Security Officers). |
| System messages | A message sent from, or addressed to, the FIN system or a SWIFT department, identified as message category 0 (for example, MT 021, MT 074). |
| T-Copy mode | A copying mode in which the service administrator, or an entity designated by the service administrator, receives a copy of all or part of the contents of a message, but plays no role in authorising or rejecting the transaction. |
| Technology and Production Committee (TPC) | A Board committee that provides technical advice and guidance to the SWIFT Board and to SWIFT Executives on the development, implementation and rollout of SWIFT solutions and services. This committee also reviews SWIFT's operational performance and technology risks in its operations and product development. |
| Technology Vendor Advisory Council (TVAC) | The forum used by the CIO to monitor and approve technology directions. |
| Test and Training (T&T) | A facility that enables users to simulate in test mode all the functions of FIN, including future message standards releases not yet available in live mode. |
| Transport Layer Security (TLS) | A cryptographic protocol which provides security for exchanging messages over a network. |
| UPS | Uninterruptible Power Supply. |
| Virtual Private Network (VPN) | A private-network capability that provides the user with dynamic allocation of resources, and a uniform numbering plan over dispersed, multiple, geographically independent locations. |
| VPN box | An IP-Sec security device installed on customer premises. The VPN box enables SWIFT to implement end-to-end security by creating and managing a secure tunnel between the customer site and the SWIFT-managed backbone access points (BAP). |
| WebAccess | SWIFT WebAccess is designed to enable secure, browser-based access from an end user who uses a standard browser, to a service provider's web server over SWIFT. WebAccess is only for person-to-application use. It is meant for use in the context of HTML-based interfaces. WebAccess provides strong user authentication to the service provider's application. It also supports the use of non-repudiated transactions (security-sensitive exchanges) when used by the service provider. |
| Y-Copy mode | A message-copying mode in which the service administrator interacts with the transaction by authorising or rejecting it before it is delivered to the intended recipient. |
| Shared Accounts | |
| Qualification Environment | A qualification environment is used to test and validate changes to a product before it is deployed in Production. |

# Appendix A: Glossary

| Term | Description |
|---|---|
| HIT Exercise | Human Intrusion Testing (or HIT Exercises) are cyber and social-engineering exercises conducted to test our physical and logical security. |

# 27 Appendix B: Mapping to CPMI-IOSCO – “Annex F”

Even though there will be always opportunities to further the advance risk management, security and resilience, SWIFT believes that overall, it meets each of the High Level Expectations:

- SWIFT meets the high-level expectation on **risk identification and management** as it has implemented appropriate policies and procedures, and has devoted significant resources in order to ensure proper governance, timely detection, follow-up and identification of mitigating actions for all risks at SWIFT.
- SWIFT meets the high-level expectation for **information security** by implementing appropriate policies and procedures and ensuring that resources are allocated to ensure the confidentiality and integrity of its information and the availability of its critical services.
- SWIFT meets the high-level expectation on **reliability and resilience** as it has implemented appropriate policies and procedures and has devoted significant resources to ensure that its critical services are available, reliable and resilient. Additionally, SWIFT’s Business Continuity Management and Disaster Recovery Plans support the timely resumption of its critical services in the event of an outage.
- SWIFT meets the high-level expectation on **technology planning** as it has implemented appropriate policies and procedures and devoted significant resources to implement effective methods and control activities to plan for the entire technology lifecycle.
- SWIFT meets the high level expectation on **communication with users** as it has implemented appropriate policies and procedures and devoted significant resources to help ensure that SWIFT: (i) is transparent to its users; and (ii) provides sufficient information enabling users to clearly understand their risk management roles and responsibilities related to their use of SWIFT.

This appendix contains a mapping table of the controls in section 1 to 5 of this report to the key questions in the “Assessment methodology for the oversight expectations applicable to critical service providers”, issued by CPMI-IOSCO in December 2014. Please note that a control is only mapped to a clarifying question if it directly relates to it. Please note that wherever the term “FMI” is used in the Key questions, this has been interpreted as “SWIFT user” for the purposes of this mapping. SWIFT users include banks, FMI’s, other financial institutions, central banks, regulators and corporate entities.

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

## 1.3 Oversight Expectation 1: Risk identification and management

**A critical service provider is expected to identify and manage relevant operational and financial risks to its critical services and ensure that its risk-management processes are effective.**

A critical service provider should have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept certain risks. A critical service provider may face risks related to information security, reliability and resilience, and technology planning, as well as legal and regulatory requirements pertaining to its corporate organisation and conduct, relationships with customers, strategic decisions that affect its ability to operate as a going concern, and dependencies on third parties. A critical service provider should reassess its risks, as well as the adequacy of its risk-management framework in addressing the identified risks, on an ongoing basis.

The identification and management of risks should be overseen by the critical service provider's board of directors (board) and assessed by an independent, internal audit function that can communicate clearly its assessments to relevant board members. The board is expected to ensure an independent and professional internal audit function. The internal audit function should be reviewed to ensure it adheres to the principles of a professional organisation that governs audit practice and behaviour (such as the Institute of Internal Auditors) and is able to independently assess inherent risks as well as the design and effectiveness of risk-management processes and internal controls. The internal audit function should also ensure that its assessments are communicated clearly to relevant board members.

| | Key question | Related controls |
|---|---|---|
| | **Enterprise-wide risk-management framework** | |
| 1.1 | What are the critical service provider's processes and systems to identify and document its risks, including relevant operational, financial, and human resources risks? What risks did the critical service provider identify and document through its processes and systems? | • 1.2.1.7-8 |
| 1.2 | What are the critical service provider's processes and systems to manage these risks? How does the critical service provider decide on accepting residual risks? | • 1.2.1.7<br>• 2.2.1.10 |
| 1.3 | How does the critical service provider reassess its risks and the adequacy of its risk-management framework in addressing the identified risks? How frequently is this reassessment conducted? | • 1.2.1.7 |
| 1.4 | How does the critical service provider address any legal or regulatory requirements or changes in requirements? | • 1.2.1.9<br>• 2.2.1.8<br>• |
| 1.5 | How does the critical service provider assess risks relating to its relationships with users? | • 2.2.10.2<br>5.2.1.3<br>5.2.3.5 |
| 1.6 | How does the critical service provider incorporate risk management into its strategic decision-making process, including assessments of general business risk and financial condition? | • 1.2.1.2<br>1.2.1.7-8 |
| | **Dependencies on third parties** | |
| 1.7 | How does the critical service provider identify and monitor the risks that dependencies on third-party providers might pose to its operations? | • 1.2.2.2-7 |
| 1.8 | How does the critical service provider assess that the security, reliability and resilience of its operations are not reduced by dependencies on third parties? | • 1.2.1.7<br>• 1.2.2.3<br>• 1.2.2.7 |

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

| | Key question | Related controls |
|---|---|---|
| **1.9** | How does the critical service provider manage/address any unaccepted reduction in the security, reliability and resilience of its operations caused by its dependencies on third parties? | • 1.2.2.1-2<br>• 1.2.2.6<br>• 2.2.1.11 |
| | **Governance of the enterprise-wide risk-management framework** | |
| **1.10** | What are the critical service provider's governance arrangements for the identification and management of risks? What are the lines of responsibility and accountability within the critical service provider, as it relates to risk management? How frequently is the effectiveness of the internal audit function reviewed? | • 1.2.1.1<br>• 1.2.1.7-8 |
| **1.11** | How does the critical service provider's board explicitly review and endorse the enterprise-wide risk-management framework? | • 1.2.1.1<br>• 1.2.1.8 |
| | **Internal audit function** | |
| **1.12** | How does the critical service provider ensure an independent and professional audit function? To which of the internationally accepted practices that govern the audit profession does the internal audit function adhere? | • 1.2.1.1 |
| **1.13** | What are the reporting mechanisms for the internal audit function to communicate its findings to the board and, where appropriate, its regulator or overseer? | • 1.2.1.1<br>• 1.2.1.5 |

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

## 1.4 Oversight Expectation 2: Information security

**A critical service provider is expected to implement and maintain appropriate policies and procedures, and devote sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil the terms of its relationship with an FMI.**

A critical service provider should have a robust information security framework that appropriately manages its information security risks. The framework should include sound policies and procedures to protect information from unauthorised disclosure, ensure data integrity, and guarantee the availability of its services. In addition, a critical service provider should have policies and procedures for monitoring its compliance with its information security framework. This framework should also include capacity planning policies and change-management practices. For example, a critical service provider that plans to change its operations should assess the implications of such a change on its information security arrangements.

| | Key question | Related controls |
|---|---|---|
| | **Information security framework** | |
| **2.1** | What is the critical service provider's enterprise-wide information security framework for providing general, overarching guidance on the solutions and practices for addressing physical and cyber security risks? How does this framework encompass policies and procedures for:<br><br>a) categorising assets (systems and services) along the dimensions confidentiality, integrity, and availability;<br>b) identifying internal and external threats on an ongoing basis;<br>c) selecting, implementing, and documenting security controls to mitigate identified risks and vulnerabilities; and<br>d) adequate governance of all security risk-management activities? | • 1.2.1.4<br>• 1.2.1.7<br>• 2.2.1.2<br>• 2.2.1.8 |
| **2.2** | How does the critical service provider incorporate relevant international, national, and industry standards into its policies and procedures? | • 2.2.1.2<br>• 2.2.1.8 |
| **2.3** | What sources of information security risks has the critical service provider identified relating to its critical services? How has the critical service provider addressed these risks? | • 1.2.1.4<br>• 1.2.1.7<br>• 2.2.1.8 |
| **2.4** | What is the critical service provider's board involvement in the critical service provider's information security framework? Does the board explicitly review and endorse the framework? How frequently does the board review the framework? | • 1.2.1.2<br>• 1.2.1.4<br>• 2.2.1.1<br>• 2.2.1.9 |
| **2.5** | How has the critical service provider's board endorsed senior management's key roles and responsibilities for information security? | • 2.2.1.1 |
| | **Information security policies and procedures** | |
| **2.6** | What policies and procedures are used to prevent unauthorized access and unauthorized disclosure of information? In particular, what are policies and procedures for:<br>a) granting authorizations to and removing authorizations from users, including both logical and physical access;<br>b) periodic recertification of user privileges;<br>c) granting, using, and controlling administrator (or highly privileged) accounts;<br>d) avoiding data confidentiality breaches;<br>e) protecting the integrity of systems against logical or physical attacks; and embedding controls in applications provided to the FMI, to prevent errors, loss, unauthorized modification, or misuse of information? | • 2.2.1.2-3<br>• 2.2.1.8<br>• 2.2.2.1<br>2.2.2.5-7<br>• 2.2.5.1-12<br>•<br>• |

# Appendix B: Mapping to CPMI-IOSCO – “Annex F”

| | Key question | Related controls |
|---|---|---|
| 2.7 | How does the critical service provider ensure that all employees and relevant external parties are made aware of their responsibilities and liabilities, and of security threats, as defined in the information security framework? | • 2.2.1.5-6<br>• 2.2.1.12 |
| 2.8 | What policies and procedures are used to ensure the confidentiality, integrity, and non-repudiation of data, including while in-transit on networks and while stored at the critical service provider? | • 2.2.1.9<br>• 2.2.4.1-8<br>• 2.2.5.5<br>• 2.2.5.7-9<br>• 2.2.5.12-13<br>• 2.2.7.2<br>• 2.2.7.4-5<br>• 2.2.10.1-10<br>• 2.2.10.12-15<br>• 2.2.10.19-22 |
| 2.9 | What policies and procedures are used to detect, react to, and recover from information security incidents? | • 2.2.1.14<br>• 2.2.5.11<br>• 3.2.1.3<br>• 3.2.1.5<br>• 5.2.2.1 |
| | **Security compliance monitoring** | |
| 2.10 | How does the critical service provider verify compliance with its information security framework and monitor the effectiveness of the security controls in place? Specifically, do these policies and procedures include vulnerability scanning and penetration testing at both infrastructure and application level? | • 1.2.1.5<br>2.2.1.2<br>2.2.1.6-7 |
| 2.11 | To what extent is the critical service provider's information security framework subject to internal and external audit? | • 1.2.1.5 |
| 2.12 | How and with what frequency is the critical service provider's board updated on the main findings of the security compliance monitoring activities? | • 1.2.1.1-2<br>• 1.2.1.5 |
| | **Capacity planning** | |
| 2.13 | What are the critical service provider’s policies on capacity planning? How does the critical service provider monitor and adjust the use of resources to meet the needs of the FMI and, where appropriate, its participants, even in stressed market conditions? How does the critical service provider address situations where the FMI’s or participant’s needs exceed operational capacity? | • 2.2.6.1<br>• 2.2.6.4-5 |
| 2.14 | How does the critical service provider review, audit, and test the scalability and adequacy of its capacity to handle, at the minimum, projected stress volumes identified by one FMI, and, where applicable, concurrent projected stress volumes when serving several FMIs? How frequently does the critical service provider conduct these reviews, audits, and tests? | • 2.2.6.1-2<br>• 2.2.6.5 |
| | **Change management** | |
| 2.15 | How do the critical service provider's change management and project management policies and procedures mitigate the risks that changes inadvertently affect the security and reliability of the critical service provider's operations? | • 2.2.8.1-14 |

# Appendix B: Mapping to CPMI-IOSCO – “Annex F”

| | Key question | Related controls |
|---|---|---|
| 2.16 | How do the critical service provider's change management policies define formal management responsibilities and procedures for the planning and testing of changes, including regression, performance and security testing? | • 2.2.8.1-14 |
| 2.17 | To what extent are changes impacting users subject to consultation with the FMI and tested with the participation of the FMI and, where appropriate, of its participants? | • 2.2.8.8<br>• 4.2.1.1 |

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

## 1.5 Oversight Expectation 3: Reliability and Resilience

**A critical service provider is expected to implement appropriate policies and procedures, and devote sufficient resources to ensure that its critical services are available, reliable, and resilient. Its business continuity management and disaster recovery plans should therefore support the timely resumption of its critical services in the event of an outage so that the service provided fulfils the terms of its agreement with an FMI.**

A critical service provider should ensure that it provides reliable and resilient operations to users, whether these operations are provided to an FMI directly or to both an FMI and its participants. A critical service provider should have robust operations that meet or exceed the needs of the FMI. Any operational incidents should be recorded and reported to the FMI and the FMI's regulator, supervisor, or overseer. Incidents should be analysed promptly by the critical service provider in order to prevent recurrences that could have greater implications. In addition, a critical service provider should have robust business continuity and disaster recovery objectives and plans. These plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption.

| | Key question | Related controls |
|---|---|---|
| | **Available, reliable and resilient operations** | |
| **3.1** | What are the critical service provider's operational availability, reliability and resilience objectives and how are these documented? How do these objectives meet or exceed the needs of the FMI and, where appropriate, of its participants? | • 3.2.3.1<br>• 3.2.3.4-5<br>• 3.2.4.1<br>• 4.2.1.1<br>• 5.2.2.2<br>• 5.2.3.3-4 |
| **3.2** | How do the critical service provider's policies and procedures support its availability, reliability and resilience objectives? | • 3.2.4.1-2 |
| **3.3** | How does the critical service provider ensure that it provides reliable and resilient operations to the FMI and, where relevant, its participants? In particular, how does the critical service provider ensure that its different operating sites have sufficiently different risk profiles? How does the critical service provider ensure that its operating sites are adequately protected against natural disasters, power failures, and adverse human actions? How does the critical service provider ensure that its backup sites have sufficient capacity to handle the critical services for a sustained period of time? | • 2.2.9.1-5<br>• 3.2.1.4-5<br>• 3.2.2.1<br>• 3.2.3.1<br>• 3.2.3.4-5<br>• 5.2.2.2-3 |
| | **Operations monitoring and incident management** | |
| **3.4** | How does the critical service provider monitor its operations? How does the critical service provider monitor whether it meets the reliability and resilience objectives of the FMI? How is this process documented and maintained? | • 3.2.1.1<br>• 3.2.3.1-2<br>• 3.2.3.4-5<br>• 5.2.3.2 |
| **3.5** | How does the critical service provider identify, record, categorize, analyse, and manage operational incidents? How are these incidents reported to senior management? How does the critical service provider keep the FMI and, where appropriate, relevant authorities, informed about such incidents? What is the process for escalating an incident into a crisis? | • 2.2.6.2<br>• 3.2.1.2-3<br>• 3.2.3.1-5<br>• 5.2.2.2<br>• 5.2.2.4-5 |
| **3.6** | What is the process for performing a post-mortem analysis of incidents, and how is this process designed to ensure identification of the root cause of incidents and to avoid recurrence in the future? What is the FMI's involvement in such a post-mortem analysis? | • 3.2.1.6 |

# Appendix B: Mapping to CPMI-IOSCO – “Annex F”

| | Key question | Related controls |
|---|---|---|
| | **Business continuity** | |
| **3.7** | What are the critical service provider's business continuity and disaster recovery objectives? How are these objectives set by the board and senior management? How frequently are these objectives reviewed by the board and senior management? | • 1.2.1.2<br>1.2.1.4<br>• 3.2.4.1 |
| **3.8** | How do the critical service provider's business continuity and disaster recovery plans ensure the timely resumption of its critical services in the event of a service disruption, including in case of a wide-scale disruption? How do these plans address potential data loss resulting from a service disruption? | • 3.2.1.3-4<br>• 3.2.2.3-4<br>• 3.2.4.1-3 |
| **3.9** | How does the critical service provider identify scenarios on potential service disruption and how is the FMI involved in this process? | • 2.2.1.8<br>• 3.2.4.1 |
| **3.10** | How does the critical service provider's business continuity and disaster recovery plans address cyber-attacks? How do these plans ensure that the critical service provider will have the ability to identify and manage the impact of a cyber-attack, including the recovery of systems after a compromise? | • 2.2.1.10<br>• 2.2.1.12<br>• 3.2.1.3<br>• 3.2.4.1-3 |
| **3.11** | What is the critical service provider's crisis communication plan to handle service disruptions? In particular, how does the plan address communications and information exchange with the FMI and relevant authorities? | • 3.2.1.3 |
| **3.12** | How are the business continuity and disaster recovery plans tested and with which frequency? Which scenarios are tested and do they include cyber-attacks? How are the FMI and, where relevant, its participants, involved in business continuity simulation tests? | • 2.2.1.8<br>• 3.2.1.5<br>• 3.2.4.2 |
| **3.13** | How are the business continuity and disaster recovery plans of the CSP regularly assessed with the FMI expectations? | • 3.2.4.2 |

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

## 1.6 Oversight Expectation 4: Technology planning

**The critical service provider is expected to have in place robust methods to plan for the entire lifecycle of the use of technologies and the selection of technological standards.**

A critical service provider should have effective technology planning that minimises overall operational risk and enhances operational performance. Planning entails a comprehensive information technology strategy that considers the entire lifecycle for the use of technologies and a process for selecting standards when deploying and managing a service. Proposed changes to a critical service provider's technology should entail a thorough and comprehensive consultation with the FMI and, where relevant, its participants. A critical service provider should regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.

| | Key question | Related controls |
|---|---|---|
| | **Policies, procedures and governance arrangements for technology planning** | |
| 4.1 | What are the critical service provider's policies, procedures and governance arrangements for technology planning? How do these policies, procedures and governance arrangements address the lifecycle for the use of technologies and the selection of new technological standards? | • 1.2.1.2<br>• 1.2.1.4<br>• 1.2.1.8<br>• 1.2.2.3<br>• 1.2.2.5<br>• 2.2.1.1<br>• 4.2.1.2 |
| 4.2 | How frequently does the critical service provider assess its technology risks? How do such assessments take into account reliability and resilience, obsolescence risks, and information security risks related to the use of its technology? How do these assessments take into account technology risks potentially affecting the FMI and, where appropriate, its participants? | • 1.2.1.2<br>• 1.2.2.3 |
| | **Policies, procedures, and governance arrangements for managing technological changes** | |
| 4.3 | What are the critical service provider's policies, procedures, and governance arrangements for implementing changes to the technologies used? How do these policies and procedures address release management, the consistent use of technology, and maintaining the security and stability of technology? | • 1.2.1.2<br>• 1.2.2.3<br>• 2.2.6.3 |
| 4.4 | How do these policies, procedures, and governance arrangements ensure that risks related to technology changes are identified and adequately mitigated, in order to avoid such changes potentially impacting the reliability and resilience of the provider's critical services? How and with which frequency does the critical service provider assess and test the processes used for implementing technological changes? | • 1.2.1.2<br>• 1.2.2.3<br>• 2.2.1.11<br>• 2.2.8.1-2<br>• 2.2.8.4 |
| 4.5 | How does the critical service provider consult with the FMI and, where relevant, its participants, in any proposed important changes to its technology that may materially affect the FMI? | • 4.2.1.1 |
| 4.6 | How does the critical service involve the FMI, where appropriate, when implementing a technology change? For example, is the FMI involved in the testing of technology changes as appropriate? | • 2.2.8.8<br>• 2.2.8.12 |

# Appendix B: Mapping to CPMI-IOSCO – "Annex F"

## 1.7 Oversight Expectation 5: Communication with users

**A critical service provider is expected to be transparent to its users and provide them sufficient information to enable users to understand clearly their roles and responsibilities in managing risks related to their use of a critical service provider.**

A critical service provider should have effective customer communication procedures and processes. In particular, a critical service provider should provide the FMI and, where appropriate, its participants with sufficient information so that users clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided. Useful information for users typically includes, but is not limited to, information concerning the critical service provider's management processes, controls, and independent reviews of the effectiveness of these processes and controls. As a part of its communication procedures and processes, a critical service provider should have mechanisms to consult with users and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or nonperforming risk controls of services. In addition, a critical service provider should have a crisis communication plan to handle operational disruptions to its services.

| | Key question | Related controls |
|---|---|---|
| | **General communication** | |
| **5.1** | What are the critical service provider's procedures and processes for communicating with users? | • 2.2.8.14<br>• 5.2.2.4-5<br>• 5.2.3.1 |
| **5.2** | What information does the critical service provider provide to the FMI and, where appropriate, its participants so that they understand their roles and responsibilities, enabling them to manage the risks related to their use of the critical service provider? With what frequency is this information reviewed? | • 5.2.1.3<br>• 5.2.3.3 |
| **5.3** | How does the critical service provider communicate to users on important changes to its operations? (See also Q.2.17, Q.4.5, and Q.4.6.) | • 5.2.2.2<br>• 5.2.3.1-2<br>• 5.2.3.6 |
| **5.4** | How does the critical service provider communicate to its users its risks analysis, including relevant operational, financial, and human resources risks? | SWIFT is overseen by its users through its governance arrangements. SWIFT does not provide risk analyses to its users. |
| | **Consultation mechanisms** | |
| **5.5** | What mechanisms are used by the critical service provider to consult with users and the broader market when needed (for example, on any technical changes to its operations that may materially affect the FMI)? (See also Q.4.5.) | • 4.2.1.1<br>• 5.2.3.5 |
| | **Communications on incidents and in crisis situations** | |
| **5.6** | How does the critical service provider inform users, where appropriate, about incidents? (See also Q.3.5.) | • 5.2.2.2 |
| **5.7** | What is the critical service provider's crisis communication plan for handling service disruptions? Does this plan involve all users and relevant stakeholders? (See also Q.3.11.) | • 5.2.2.6 |

# Appendix C: Management Response to Exceptions

To provide transparency to the readers of this report, this section discusses the nature of some of the exceptions and what actions are being taken or initiated to respond to these exceptions.

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| 1.2.1.7 | SWIFT conducts background in-employment and in-assignment rescreening, which is subject to local laws and regulations, and is applicable to all SWIFT employees and temporary SWIFT personnel with access to SWIFT locations and/or systems. | • For 21 out of 43 temporary personnel, in-assignment rescreening was not performed within the time limits specified by SWIFT processes.<br>• For 8 out of 40 SWIFT employees, in-employment rescreening was not performed within the time limits specified by SWIFT processes. | **Context**<br>All issues identified were in the rescreening process which is above and beyond the standard pre-employment screening that had no exceptions for 2020. Management has taken action to automate reminders and clarify escalation paths for delays.<br>**Action Plan**<br>By end of Q2 of 2021, Management will:<br>• enforce that requests for access badges will not be renewed without valid screening or for a limited (14-day grace period) exception request with risk ownership held by the line manager;<br>• implement a supervisory control dashboard; and<br>• amend the Master Service Agreement (MSA) template to include revised screening guidelines. |
| 2.2.1.18 | Passwords for privileged accounts must be transferred to and controlled by the Identity and Access Management group after system deployment. All accounts are documented for each particular service. | We noted that for 2 out of 30 sampled hosts:<br>• On 1 host, the password of a privileged account was not transferred to and controlled by the Identity and Access Management group after system deployment. | **Context**<br>The root cause has been identified within the new system process.<br>**Action Plan**<br>Management has addressed the specific exceptions and is taking action to re-inforce the transfer of hosts to Identity & Access Management during the handover |

# Appendix C: Management Response to Exceptions

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| | | • On 1 host, the audit trail demonstrating that privileged accounts were onboarded in the Identity and Access Management system after system deployment, was not available. | process enabling privileged account management as per logical access policy. |
| 2.2.1.19 | Password-protected screensavers are automatically activated on Windows workstations after a pre-set period of inactivity. Monitoring workstations residing in computer rooms and Central Control Centres where screensavers would interfere with their operational purpose are excluded. | We noted for 14 out of 30 sampled workstations:<br>• On 8 out of 30 workstations, it could not be confirmed that the global policy related to password-protected screensavers was enforced as the workstations were decommissioned.<br>• On 6 out of 30 workstations, the global policy related to password-protected screensavers was not enforced. | **Context**<br>Screensaver is enforced automatically by the central directory server. In some cases, sufficient evidence could not be provided to show that the automation successfully enforced on the end point. This was due to the end point no longer being in use or collecting appropriate evidence could have impacted operational activities. Management is taking action to archive appropriate evidence of screensaver enforcement.<br>**Action Plan**<br>Management will determine a technically feasible approach to avoid impact to operators in production, striking a balance between practicality and reasonable assurance that this control is implemented. |
| 2.2.1.26 | Security baselines stipulate configuration requirements for server and workstation operating systems. These baselines define operating system level controls that include:<br>• Directories and file protection; and<br>• Logging and auditing. | For 8 out of 30 sampled workstations and servers, the security baseline compliance was not verified during the bi-annual checks. | **Context**<br>Of the 8 systems identified<br>• 1 system was experiencing operational issues during audit period<br>• 5 systems had automated enforcement of the baseline but a sample based approach for verifying was not sufficiently documented |

# Appendix C: Management Response to Exceptions

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| | Acceptance testing verifies security baseline compliance of tested releases.<br><br>Security baseline compliance is verified for the production environment at least twice a year, with the exception of the verification of network routers and switches, which is performed yearly. Any deviations are identified and followed up through to resolution via a change request or waiver. | | • 2 systems had only a single run for the year instead of the committed 2 per year<br><br>**Action Plan**<br><br>Management will further strengthen supervisory oversight to monitor the status of the Security Baseline Compliance reviews and appropriately document varying approaches to baseline verification (such as documenting a clear escalation path if MSBs are delayed, documenting the approach for verifying MSB compliance on Windows). |
| 2.2.1.23 | Production privileged account passwords are managed according to defined requirements for length, complexity, change on use, and adhering to a minimum change frequency when unused. | For 1 out of 35 sampled production hosts the minimum password change frequency requirement was not enforced for a production privileged account. | **Context**<br><br>The password requirement was not met on the same host that was not correctly onboarded by the Identity and Access Management group per exception 2.2.1.18 above.<br><br>**Action Plan**<br><br>Corrective actions identified for that exception will also address this exception. |
| 2.2.6.17 | Anti-virus software is installed and virus signatures are kept up to date on Windows workstations and servers to prevent and detect the presence of known virus/malware. The usage of USB devices on the Windows physical workstations and Thin Clients is restricted. Deviations on the usage of USB devices is authorized as per process through a maintained list with the granted exceptions. Non-compliant systems are identified and reported to system owners and line management for follow-up. | For 5 out of 30 sampled production Windows workstations and servers, the anti-virus signatures were not kept up to date. | **Context**<br><br>The 5 systems identified were not accessible nor visible on the network.<br><br>• 2 hosts were on a fully isolated network not connected to the Production LAN, nor any external network<br><br>• 2 hosts were fully decommissioned<br><br>• 1 host was not yet connected to the network<br><br>**Action Plan** |

# Appendix C: Management Response to Exceptions

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| | | | Management has taken action to track and report all systems that are non-compliant and need follow-up. A bi-weekly sync meeting between involved teams is organised.<br><br>By end of September, Management will<br>• enable sufficient monitoring capabilities to ensure a timely and consistent follow-up of non-compliant systems as per process;<br>• implement a monthly supervisory control providing a compliance status overview to the appropriate management level(s); and<br>• ensure to maintain a complete and accurate host list containing all hosts in scope of this control. |
| 2.2.6.19 | There are software integrity checking mechanisms in place on the SWIFTNet and FIN messaging production systems. These mechanisms regularly verify the integrity of the key executables and configuration files. | We noted that 4 out of 25 sampled FIN and SWIFTNet production messaging systems were not monitored for software integrity. | **Context**<br><br>The 4 systems identified experienced operational issues that were under investigation. Management is taking action to further strengthen supervisory oversight and enforce strict resolution timers.<br><br>**Action Plan**<br><br>By end of March 2021, Management will:<br>• resolve the issues identified or submit a Security Exception Request;<br>• further enhance supervisory control through weekly visibility on agent issues; and<br>• establish SLA timers for resolving issues or creating a Security Exception Request. |

# Appendix C: Management Response to Exceptions

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| 2.2.6.5 | The development methodology defines standards for functional requirements specification, design specification and testing, which can be verified by quality assessments, quality transition checkpoints and product testing. The required evidence is reviewed and approved by the relevant stakeholders as per the development methodology. | We noted that the design specification was reviewed but not approved prior to deployment for 1 out of 11 sampled SWIFTNet software releases that were deployed in production. | **Context**<br>The exception happened during 1 of the 11 review cycles which took place in 2020 for the SWIFTNet platform. The review of the document and the tests of the software changes were properly conducted but the proper approval was missed at the end of the review process. Management has taken action to address the issue by approving the changes during the following review cycle.<br>**Action Plan**<br>Management has updated their process to ensure that design documentation is approved prior to deployment.<br>Based on evidence provided, Internal Audit has closed the issue. |
| 2.2.1.10 | Vulnerabilities identified for COTS and Open Source products are identified through scanning and intelligence feeds at least monthly. These vulnerabilities are evaluated for potential impact to SWIFT applications and services. Vulnerabilities are assigned a priority and possible remediation actions are identified. Security updates are installed in line with the requirements defined in SWIFT's Standards for Security Patching. Patching prioritization is based on vulnerability severity and exposure of the system. | We noted that:<br>• For 3 out of 35 sampled hosts, vulnerability scanning was not performed within the frequency specified by SWIFT's processes.<br>• For 8 out of 115 sampled hosts, security updates were not installed within the time limits specified by SWIFT policies. | **Context**<br>3 of the identified systems were part of network that had air gap isolation as a primary control.<br>8 of the systems identified were internal systems that had security updates beyond the required patching date. None of the sample hosts had externally facing vulnerabilities beyond patching timers.<br>**Action Plan**<br>Management performed a risk assessment to determine the appropriate controls to implement for the SCADA network. Based on the outcome of this assessment, Management updated the Standard for Security Patching. |

# Appendix C: Management Response to Exceptions

| Reference | Control Description | Exception(s) | Response(s) |
|---|---|---|---|
| | | | Per the evidence provided, Internal Audit closed the issue. |
| 3.2.1.7 | The SWIFT.com environment is deployed in two sites. | We noted that 1 out of 3 sampled servers in the swift.com environment was only deployed at one site. | **Context**<br>The Virtual Machine (VM) request did not include the requirement for dual site deployment.<br>**Action Plan**<br>Management has:<br>• updated the Virtual Machine creation form to include the proper hosting location requirements;<br>• reviewed the list of systems and their location; and<br>• corrected OLCS Virtual Machines as well as some other ones that were incorrectly configured.<br>Based on these corrective actions taken, Internal Audit closed the issue. |