White paper

Consistent and objective assurance enables compliance

CPSS-IOSCO'S Principles for Financial Market Infrastructures (FMIs)

How a coherent assurance framework for critical service providers helps FMIs to assess and disclose compliance.

Highlights

- CPSS[1]-IOSCO[2] raise the bar for financial market infrastructures and their critical service providers to help achieve effective risk management, strong governance and oversight
- Compliance may have to be demonstrated as of 2013
- SWIFT proposes industry-wide adoption of a consistent and robust assessment and disclosure framework for critical service providers, based on international assurance standards and requiring external independent validation
- SWIFT confirms compliance with the expectations for critical service providers

A coherent assurance framework for Critical Service Providers will facilitate the assessment and disclosure of FMIs' compliance with the new principles for FMIs from CPSS-IOSCO

Executive Summary

Financial Market Infrastructures ("**FMIs**") are important contributors to the removal of financial risks but must ensure that they do not themselves become sources of unacceptable risk in the financial system, particularly in severe stress conditions. As FMIs often rely on the services of third-parties for essential aspects of their service, these Critical Service Providers ("**CSPs**") play an important role in the mitigation of the FMIs' operational risks.

To foster effective risk management, strong governance and oversight of FMIs, CPSS[1] and IOSCO[2] have issued new Principles for FMIs[3] ("**Principles**"): a set of broad governance, business and operational standards that significantly raise the bar on compliance expectations for FMIs and their CSPs. These expectations establish a "standard of use" by setting a minimum baseline in the areas of risk identification and management, information security, reliability and resilience, technology planning and communication with users.

CPSS and IOSCO members will strive to adopt the Principles by the end of 2012 and put them into effect as soon as possible. FMIs are expected to observe the standards as soon as possible.

In 2007, the G-10 central bank overseers of SWIFT introduced the High Level Expectations ("**HLEs**") to structure the oversight of SWIFT. The HLEs cover the same aspects as the expectations for CSPs and since 2007 SWIFT has provided its overseers an annual self-assessment against these HLEs[4]. Given the similarities between the two frameworks and a long history of self-assessment, already today, SWIFT is confident that it complies with the oversight expectations for critical service providers. We will disclose compliance under the proposed assurance framework outlined below. SWIFT is convinced that FMIs will greatly benefit obtaining from all their CSPs such third party assurance on compliance with the Expectations, in addition to any self-assessment that CSPs may have undertaken.

[1] Committee for Payment and Settlement Systems, Bank for International Settlements

[2] International Organization of Securities Commissions

[3] Principles for financial market infrastructures, CPSS-IOSCO, April 2012 (http://www.bis.org/publ/cpss101a.pdf)

[4] The assessment methodology introduced by SWIFT as a response to the Expectations is without prejudice to the prerogatives of the overseers of SWIFT to determine the oversight policy vis-à-vis SWIFT.

Complementing the assessment and disclosure framework for FMIs proposed by CPSS-IOSCO for FMIs' compliance with the Principles, SWIFT proposes a scalable, cost-efficient and coherent assurance framework based on internationally accepted assurance standards that require independent external validation of the CSPs' conformance with the new oversight expectations.

Introduction

Raising the bar – The CPSS-IOSCO recommendations for FMIs

FMIs are considered vital to the safety, security and stability of the financial markets and the global financial system. Regulatory authorities see FMIs as important contributors to the removal of some of the risks that exacerbated the financial crisis. At the same time, authorities are focused on ensuring that FMIs do not themselves become sources of unacceptable risk in the financial system. Recent legislation in major markets[5] compels market participants to use FMIs for an increasingly wide range of transactions e.g., Dodd-Frank in the US and the European Market Infrastructure Regulation (EMIR) in the EU.

As a result and in support of the initiative of the Group of Twenty Finance Ministers and Central Bank Governors and the Financial Stability Board to strengthen core financial infrastructures and markets, two key regulatory organizations – CPSS and IOSCO – have reviewed and updated the existing standards[6] for FMIs and defined a set of principles to minimize the risk of FMI failure.

The Principles are wider in scope, incorporate lessons learned from the financial crisis and take into account the experience of implementing the existing standards during the past years – effectively raising the bar for FMIs and their service providers. Following a consultation in 2011, CPSS-IOSCO published the final set of 24 principles for FMIs on 16 April 2012.

General applicability of principles to specific types of FMIs

Principle	PSs	CSDs	SSSs	CCPs	TRs
1. Legal basis	•	•	•	•	•
2. Governance	•	•	•	•	•
3. Framework for the comprehensive management of risks	•	•	•	•	•
4. Credit risk	•		•	•	
5. Collateral	•		•	•	
6. Margin				•	
7. Liquidity risk	•		•	•	
8. Settlement finality	•		•	•	
9. Money settlements	•		•	•	
10. Physical deliveries		•	•	•	
11. Central securities depositories		•			
12. Exchange-of-value settlement systems	•		•	•	
13. Participant-default rules and procedures	•	•	•	•	
14. Segregation and portability				•	
15. General business risk	•	•	•	•	•
16. Custody and investment risks	•	•	•	•	
17. Operational risk	•	•	•	•	•
18. Access and participation requirements	•	•	•	•	•
19. Tiered participation arrangements	•	•	•	•	•
20. FMI links		•	•	•	•
21. Efficiency and effectiveness	•	•	•	•	•
22. Communication procedures and standards	•	•	•	•	•
23. Disclosure of rules, key procedures, and market data	•	•	•	•	•
24. Disclosure of market data by trade repositories					•

Source: CPSS-IOSCO Principles for Financial Market Infrastructures, April 2012

While some of the principles only apply to particular types of FMIs, a number of them – such as legal and governance issues – apply to all. Also applicable to all types of FMIs is Principle 17 on operational risk. Amongst other things, Principle 17 requires FMIs to manage the risks service providers might pose to their operations.

In addition to these Principles that will allow monitoring the level of risk management across FMIs, CPSS-IOSCO also published for consultation the Assessment methodology for the principles for FMIs and the responsibilities of authorities and the Disclosure framework for financial market infrastructures. The assessment methodology provides a framework for assessing the observance of the principles ensuring objectivity and comparability across all relevant jurisdictions. The disclosure framework promotes coherent disclosure of information by FMIs giving a clear understanding of the FMI's operations and its impact on participants and the market it serves. The assessment methodology and disclosure framework cover the Principles, but not the expectations for CSPs. The assessment methodology proposed by SWIFT extends the advantages of objectivity and comparability across all CSPs serving the FMIs.

CPSS and IOSCO members will strive to adopt the Principles by the end of 2012 and put them into effect as soon as possible. FMIs are expected to observe them as soon as possible following regulatory implementations, and CPSS-IOSCO will be setting up an assessment committee to monitor progress.

[5] See also "Facing the unknown: Building a strategy for regulatory compliance in an uncertain landscape", August 2012, (http://www.swift.com/resources/documents/Regulation_white_paper.pdf)

[6] Examples are:

(1) CPSIPS (January 2001), the CPSS ten principles define how systemically important payment systems should be built and regulated globally;
(2) RSS (November 2001), 19 recommendations for promoting the safety and efficiency of SSS; and,
(3) RCP (November 2004), 15 recommendations addressing the major risk that CCPs face

Establishing the baseline – The expectations for all CSPs included in the Principles

FMIs have always had commercial reasons for closely monitoring the effectiveness of all of their CSPs as part of their overall risk management strategy, as service reliability and robustness have become vital in the increasingly demanding and competitive market in which FMIs operate. These commercial drivers are now enhanced and reinforced by regulatory requirements. Whilst the Principles are directed at all FMIs, their reach goes further and impacts those organizations that provide critical services to FMIs.

The operational reliability of an FMI may be dependent on the continuous and adequate functioning of service providers – e.g., third party technology and messaging providers – that are critical to an FMI's operations. CSPs are highly relevant in terms of the potential contribution they make to the ability of FMIs to ensure smooth operation of their mission-critical systems and to comply with Principle 17 on operational risk. Recognizing the important role of CSPs in relation to operational risk, the Principles define the Expectations for CSPs ("**Expectations**") in "Annex F" of the document issued by CPSS-IOSCO in April. Annex F starts from the premise that the operational activities performed by a CSP need to be held to the same standard as if the FMI were performing the operation itself.

The Expectations outlined in Annex F set "standards of use" in the following areas:

1. Risk identification and management, to control relevant operational and financial risks;
2. Information security, to secure efficient policies for the confidentiality and integrity of information;
3. Reliability and resilience, to ensure high availability, reliability and resilience;
4. Technology planning, to confirm robust methods are in place to plan technology selection and use;
5. Communication with users, to enable clear communication with the FMIs to understand risk management on critical services.

These Expectations are written at a broad level, allowing CSPs flexibility in demonstrating that they meet the expectations.

The FMIs subject to the Principles will be increasingly compelled to assess and report to FMIs on their CSPs against the criteria laid down in the Expectations. This requirement for the FMIs will be greatly facilitated if they can count on assessment reports made available by their CSPs. Further efficiency can be achieved if all CSPs prepare such reports along a consistent methodology, and if the assurance is provided by the involvement of an independent, external party. CSPs may also be required to report directly to the regulators. There is a clear trend of increasing focus on risk management in legislation relevant to FMIs currently being developed in some markets, e.g. the Central Securities Depositories Regulation and EMIR regulations in the EU.

Take away #1

"A uniform, standardised assessment and disclosure methodology with external validation by qualified assessors is the best way to ensure effective, efficient and transparent compliance for all stakeholders – Regulators, FMIs and CSPs"

SWIFT as a CSP to FMIs

The principles apply to payments systems, central clearers, securities depositories and settlement systems, as well as trade repositories. SWIFT plays a key operational role for all of these categories of FMIs in markets across the globe: SWIFT is for many FMIs a key provider of messaging services, linking the FMI to its user community. For others, SWIFT acts as a provider of infrastructure hosting services. With SWIFT being the service provider of choice for many FMIs across the globe, SWIFT clearly fits the definition of a CSP and hence needs to demonstrate compliance with the Expectations.

From its inception, SWIFT has been heavily focused on risk management, operational excellence and constructive dialogue with its stakeholders. SWIFT has already performed a self-assessment against the Expectations. Appendix A summarises the results of SWIFT's existing self-assessment against the Expectations as we have been subject to similar requirements since 2007. We have also included a list of key controls that help SWIFT meet or exceed the Expectations. Going forward however, and as the Expectations will apply to all CSPs as of 2013, SWIFT is of the opinion that such self-assessment is not sufficient, but that a coherent assessment methodology is required which includes external validation for all CSPs. The addition of external validation will improve consistency and transparency. Because of the harmonised assessment methodology, there will be efficiency gains for the FMIs and regulatory authorities that receive the reports. SWIFT will adopt the new proposed assurance methodology as from 2013.

A Common Assurance Framework for CSPs

While many FMIs already have bespoke assurance arrangements with their CSPs, the publication of the CPSS-IOSCO guidance now creates a regulatory obligation for all FMIs across the globe to actively seek confirmation that their CSPs have implemented robust processes that withstand scrutiny in all areas covered by the Expectations.

Take away #2

"If FMIs rely on third parties for vital aspects of their mission-critical systems, it is crucial these dependencies are identified and that independent assurance is obtained on the CSPs' full compliance with the Expectations"

Given its criticality for the global financial community, its experience in standardisation, and its transparency on risk identification and management, information security, reliability and resilience, technology planning and communication with users, SWIFT has established over the years a widely accepted assurance framework to address the assurance requirements from the SWIFT community and the G-10 Central Banks that oversee SWIFT. Building on this experience and expertise, SWIFT has now built an enhanced assurance framework to demonstrate compliance with the Expectations.

The development of this framework was driven by six key requirements:

1. To facilitate global acceptance and adoption, the framework must be **based on internationally recognised assurance standards;**
2. To maximise the value of the assessment, the framework must include **validation of conformance by a qualified, independent external assessor**. The independent assessor's opinion must cover both the adequacy of control design and the operating effectiveness of the controls;
3. To ensure continued focus, the assessment must be **timely and periodically updated**;
4. To be a realistic solution, the framework must allow the assessment and disclosure to be **scalable**, with efforts proportionate to the size of the CSP, but without reducing the rigour and completeness of the assessment;
5. To be cost-effective, the framework must **allow leveraging existing assurance work** that meets the minimum quality requirements; and,
6. To be future-proof, the assurance framework needs to be **flexible** and remain valid even if the assurance requirements are updated in the future.

An assurance framework that satisfies these requirements will allow the FMI to inform the relevant authorities about the performance of the CSPs, or for the CSPs to report directly to those authorities, as required by Principle 17.

SWIFT strongly recommends that this methodology be adopted by all FMI CSPs to help provide a coherent and objective assurance process for all CSPs to FMIs worldwide.

An international standards-based assurance framework for all CSPs

To ensure consistency over time and amongst jurisdictions, the choice of an appropriate and internationally recognised assurance standard is vital.

SWIFT proposes assessments be performed under the International Standard on Assurance Engagements ("**ISAE**") 3000. This standard deals with assurance engagements other than audits or reviews of historical financial information. It is a principles-based standard that is capable of being applied effectively to a broad range of underlying subject matters. It is proposed that this framework be used for a "reasonable assurance attestation engagement" whereby the auditor provides an opinion on the adequacy and effectiveness of the controls based on assurance work performed. The nature, timing and extent of the procedures performed must be planned to result in a level of assurance that is, in the auditor's professional judgment, meaningful to the intended users.

In practice this will mean that an audit professional will provide an opinion on whether the organizational units, policies, procedures and user responsibilities achieve the required expectations in the areas of risk identification and management, information security, reliability and resilience, technology planning and communication with users, and that these controls were effective in the reporting period (typically the preceding calendar year).

The proposed framework recognizes that CSPs may already have assurance mechanisms in place. To the extent that these assurance mechanisms are standards-based (e.g., ISAE 3402) and relevant, the audit professional can incorporate the conclusions or assurance work already performed as long as the requirements of ISAE 3000 are satisfied.

A single uniform assurance methodology will benefit all stakeholders – FMIs, CSPs and regulators – as this will:

1. enable a coherent and objective approach to be adopted for operational compliance by FMIs;
2. clarify assurance expectations for CSPs and this will allow them to operate in a level playing field;
3. maximise the effectiveness of the review of operational risk by regulators, both in their assessment of the FMIs and of the FMI's dependency on CSPs; and,
4. facilitate assessment of an FMI's operational risk by regulators.

Providing comfort to the FMIs – Verification of Compliance

The achievement of the objectives of the Principles and more specifically the Expectations depends on the continuous and adequate functioning of service providers that are critical to an FMI's operations. As the operational reliability of an FMI may be dependent on the continuous and adequate functioning of their CSPs, SWIFT strongly recommends that the assessment of a CSP's adherence to the Expectations be performed by qualified independent assurance professionals.

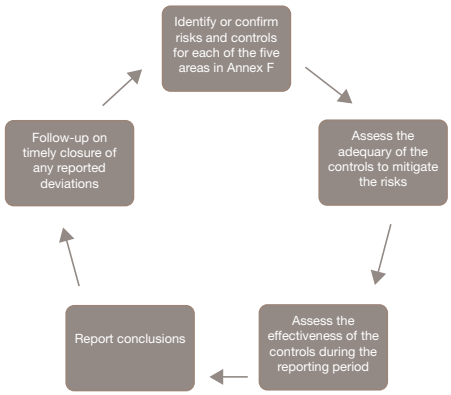
Take away #3

"A single uniform assurance methodology will benefit all FMIs, CSPs and regulators"

Providing timely assurance – Continuous monitoring and periodic reporting

To help ensure timely updates of the initial assessment, the assurance process must be based on the continuous monitoring of compliance with the stated objectives and be driven by a desire for constant improvement of the control activities.

A typical frequency to reassess CSP's compliance with the Expectations would be annual, and preferably by calendar year.



Typical annual assurance activities

Conclusion

FMIs are critical components of the financial ecosystem. They can bring stability in market stress situations but could also be a conduit for financial shocks if risks are not well managed. CSPs have a key role to help FMIs to limit their operational risks.

The Principles and the accompanying Expectations significantly step up the assurance requirements for both FMIs and their CSPs.

In response to the Expectations, we propose an enhanced assessment and disclosure framework based on international assurance standards with the compliance validation performed by independent, qualified assessors. This assurance framework has value well beyond SWIFT and the FMIs using SWIFT as a CSP as it provides a basis for a common assurance standard that can be used by all FMIs for all their existing or future CSPs. The benefits to FMIs, CSPs and regulators of the industry-wide adoption of this enhanced assessment and disclosure framework are compelling:

— The consistency of the assurance reporting will allow FMIs (and their regulators) to compare performance of CSPs against the expectations in the areas of risk identification and management, information security, reliability and resilience, technology planning and communication with users. This will help enhance market transparency and promote a common level of observance of the Expectations;
— With the quality requirements built in to the international assurance standard, the methodology ensures a level playing field for all CSPs; and,
– The framework is future proof. Even if CPSS-IOSCO chooses to change the assessment and framework for CSPs and implements a more centralised follow up, the work done by CSPs remains valid.
— The framework is scalable, minimizes the total cost of ownership of CSPs' regulatory response and is cost-efficient for FMIs and regulators.

We believe these benefits are enticing arguments for the proposed assessment and disclosure approach to be adopted by all FMIs and CSPs.

Appendix A shows that SWIFT has already performed a self-assessment and can confirm compliance with all expectations for CSPs. It also shows how SWIFT has embraced the proposed new framework and is preparing to issue the first resulting assurance report in 2013.

Appendix A

Summary of SWIFT's Current Self Assessment[7] against the five oversight expectations applicable to Critical Service Providers published in CPSS-IOSCO Principles For FMIs, Annex F

SWIFT's Self-Assessment of Compliance with the Oversight Expectations for CSPs

SWIFT has put in place service commitments, an organisational structure, policies, procedures, processes, control activities, and independent review bodies and activities to help ensure we achieve our corporate objectives in terms of providing secure, reliable and scalable financial messaging services for the financial community as a whole, as well as our customer and oversight expectations for critical service providers. For the same reason, we have also clearly delineated our responsibilities, as well as those of SWIFT users.

These key controls not only help us to demonstrate that we effectively meet the oversight expectations relevant to critical service providers; they also help ensure we remain the preferred global provider of secure financial messaging services of the financial community.

SWIFT challenges itself to continuously improve its delivery of services to its customers and in doing so to address the inevitable changes to the world in which we operate. This work includes continuing improvements to SWIFT's resilience and security to benefit our customers in the global financial community. Even though there will always be opportunities to further advance our risk management, security, and resilience.

Take away #4

"Based on self assessment and subject to external validation in 2013, we believe that overall SWIFT meets each of the oversight expectations applicable to critical service providers"

Below we summarise the five oversight expectations applicable to critical service providers, as well as SWIFT's current self-assessment against them. It should be noted that while these results are presented as a self-assessment, many of the controls are also part of SWIFT's most recent (2011) ISAE 3402 report that includes PricewaterhouseCoopers' unqualified opinion. This report is available to SWIFT users on request via www.swift.com | About SWIFT | Publications | Information Security, or by sending an e-mail to ISAE_3402@swift.com.

In line with the arguments in this paper, SWIFT will enhance this self-assessment and implement the proposed standard assessment and disclosure process using an external assessor as of 2013. SWIFT advocates that such third party assurance on compliance with the expectations for CSPs should be obtained for all CSPs, in addition to any self-assessment that CSPs may have undertaken.

1. Risk Identification and Management

High Level Expectation

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 on-going 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.

[7] As per the proposed methodology, the results of SWIFT's self-assessment will be subject to external validations as of 2013.

Result of Self-Assessment

SWIFT meets the high-level expectation on risk identification and assessment 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.

Specifically,

- SWIFT has mature processes in place to identify, manage, mitigate and revisit security, technology, financial and vendor related risks. For example: SWIFT monitors its dependence on third parties – this includes monitoring the financial health of key suppliers, as well as reviewing the technology obsolescence risks. SWIFT's Legal department regulates the legal and regulatory developments on specific relevant topics in the major jurisdictions where SWIFT operates;
- The Board has proper, adequate supervision over activities in order to monitor and manage risks, including strategic decisions that impact long-term continuity of SWIFT services. The Board is informed of the risks on a regular basis;
- The Chief Risk Officer (CRO) is responsible for ensuring compliance with the risk management framework. In conjunction with the CEO and the Executive Committee, he develops and communicates risk management policies, risk appetite and risk limits. The CRO is also responsible for establishing and communicating the overall ERM objectives and direction, as well as for implementing appropriate risk reporting to the Board, CEO, Executive Committee, senior management and Oversight. The CRO reports to the Chief Financial Officer (CFO) with unrestricted access to the Board's Audit and Finance Committee (AFC);
- SWIFT has a strong, independent Internal Audit group which reports directly to the AFC as well as the Chief Executive Officer (CEO). The Internal Audit group is organised to match best-in-class international practices as prescribed by the Institute of Internal Auditors, including independence and professional standards. The Audit Manual formalises the audit process from annual planning to issue follow-up. The Internal Audit group has a strong quality assurance program and is reviewed by an independent third-party against relevant international professional standards; and,
- All of the aforementioned processes are subject to independent audit review on a rotational basis, either by Internal Audit or by the External Auditors. Internal Audit's Audit Universe includes ERM and Security Risk Management (SRM), as well as all other risk management functions and processes at SWIFT.

2. Information Security

High-Level Expectation

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.

Result of Self-Assessment

SWIFT has met 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.

Specifically,

- SWIFT has a Security Strategy, Security Control Framework and Security Policy, which set out the high-level principles for confidentiality, integrity and availability. Further practical advice is provided in the Security Standards. Where more detailed advice for implementation of controls is warranted, further guidance for practical implementation is provided in procedures;
- Management operates a set of supervisory controls to monitor compliance with standing policies;
- Security Compliance Management ensures effective and continuous compliance monitoring and reporting. As of 2007, compliance monitoring and reporting was expanded to include control statements from selected policies;
- SWIFT's capacity planning process allows proactive and long term planning of system deployment, while continuously following up on the status of network usage, system behaviour, traffic flow performance and customer service level adherence. The capacity planning process includes end-user implementation capacity planning, system capacity planning and network capacity planning;
- SWIFT has formal change management policies and procedures, which evaluate the impact of any change before implementation; and,
- Internal Audit, External Security Audit and External Financial Audit independently review compliance with standing policies and procedures.

3. Reliability and Resilience

High-Level Expectation

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.

Result of Self-Assessment

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.

Specifically,

- SWIFT maintains multiple Operating Centres that all have sufficient capacity to process peak volumes. Based on defined Recovery Time Objectives (RTO) for internal and external services, SWIFT has implemented and exercises Disaster Recovery and Business Continuity Plans. The RTOs are defined on the basis of applicable data classification and service commitments;
- Depending on their criticality, the infrastructure supporting SWIFT's services can be spread over multiple Operating Centres. SWIFT also maintains and tests a dedicated Disaster Recovery Infrastructure (DRI) designed to make its critical services available to the SWIFT community, in case services could not be provided from the regular operating environment;
- SWIFT has multiple Customer Support Centres (CSCs), located on different continents, with procedures in place to redirect incoming customer requests to other CSCs, should this be required;
- Disaster Recovery and Business Continuity Plans are exercised with predefined frequencies, reflecting the criticality of the service. The scheduled tests include: general service continuity tests, DRI activation tests, site takeover tests, and floor down tests. SWIFT's top customers (Critical Customer Locations) are invited to participate in the DRI activation testing. Customer participation allows SWIFT to test the customer's ability to resume business once the service has been re-established;
- SWIFT monitors its Production services 24x7. Processes and procedures are in place to detect, record, report and escalate problems to ensure they are resolved in a timely fashion. Management has supervisory controls in place to ensure the Problem and Incident Management Processes work as designed. Critical operational problems are reviewed to identify root causes; processes are in place to monitor the implementation of actions based on lessons learned; and,
- Internal Audit reviews the Business Continuity Process and Procedures, as well as the Problem and Incident Management Process. These processes, as they apply to the SWIFTNet and FIN services, are also in scope of SWIFT's annual ISAE 3402 Report. Additionally, Internal Audit observes the major Business Continuity testing exercises.

4. Technology Planning

High-Level Expectation

The critical 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.

Result of Self-Assessment

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 and technological standards selection.

Specifically,

- The mission of IT is to support the business (priorities are expressed in the 5 year strategic plan and the annual operating plans). All technology and standards choices are made in this context;
- There is proper governance of these processes by the Board (Audit and Finance Committee and Technology and Production Committee) and the Executive Committee (ExCo);
- The Board's Technology and Production Committee (TPC) is regularly updated on the current evaluation of the technology deployed at SWIFT;
- The Technology Vendor Advisory Council (TVAC) meets regularly to assess technology used at SWIFT;
- Management has supervisory controls in place to ensure the Technology Planning Processes work as designed; and,
- Internal Audit reviews the Technology Planning processes. These processes, as they apply to the SWIFTNet and FIN services, are also in scope of SWIFT's annual ISAE 3402 Report.

While we have appropriate and effective processes in place to ensure alignment of the IT strategy with the SWIFT strategy, these processes are not formalised in process documents.

5. Communication with users

High-Level Expectation

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 non-performing risk controls of services. In addition, a critical service provider should have a crisis communication plan to handle operational disruptions to its services.

Result of Self-Assessment

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.

Specifically,

- Services Descriptions and Product Documentation clearly stipulate user responsibilities;
- SWIFT has both permanent and ad-hoc consultation processes in place that ensure that customer concerns regarding business and technology are considered; and
- Support Service Descriptions describes the support levels available to SWIFT customers and comprehensively describes the types of communication used.

For more information about SWIFT
visit swift.com

To join the community debate
visit swiftcommunity.net

Legal Notices

Contacts:

Peter DE KONINCK
Deputy Chief Auditor, Internal Audit
+ 32 2 655 4217
peter.dekoninck@swift.com

Stephane Ernst
Global Head of High Value Payment
Market Infrastructures Marketing
+32 2 655 3328
stephane.ernst@swift.com

Richard Young
Regulatory Affairs
+44 20 7762 2029
richard.young@swift.com