SWIFT’s response to the joint Bank of England’s, Prudential Regulation Authority’s and Financial Conduct Authority’s discussion paper on Building the UK Financial Sector’s Operational Resilience

SWIFT

05 October 2018

Confidentiality: Public

SWIFT thanks the Bank of England, Prudential Regulation Authority and Financial Conduct Authority for the opportunity to provide comments on the discussion paper on Building the UK Financial Sector's Operational Resilience. While SWIFT is neither a financial market infrastructure, nor a financial institution, we appreciate the opportunity to provide feedback on this important subject.

SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT's messaging services are designed to be available 24 hours a day, 365 days a year, with some limited planned downtime. They support more than 11,000 financial institutions around the world and have systemic importance for the global economy; our users trust us to deliver. As a critical technology and infrastructure provider, our objective is to ensure that our systems work securely and reliably every day, while remaining alert to new threats and opportunities.

The expertise and dedication of our staff, our long-term technology investment and renewal programmes, and our constant vigilance towards new threats, are key components in ensuring we meet this challenging commitment, day after day, year after year.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Marcel Bronmans
SWIFT | Chief Operations Officer
Tel: +32 2 655 3511
www.swift.com

CHAPTER 2: OPERATIONAL RESILIENCE OF BUSINESS SERVICES

Question A): What are readers' views on the proposed focus on continuity of business services? Would a service rather than systems-based approach represent a significant change for firms and FMIs compared with existing practice? What other approaches could be considered?

SWIFT response:

The supervisor's proposed focus on continuity of business services is the correct approach. In today's environment, it is vital to safeguard effectively against operational disruptions and manage related risks. Indeed the Business Continuity standard ISO 22317 states: "As the first step in the business impact analysis process, the organization's top management should agree on the priority of *products and services* following a disruptive incident which may threaten the achievement of their objectives."

At SWIFT, this approach would not mean significant changes as our focus is on ensuring the continuity of our business services, and our Business Continuity Framework is already aligned with the Business Continuity standard ISO 22317. We have found this approach to be the best way of identifying which IT systems have the highest priority – something a 'bottom-up' approach does not properly reveal. In turn this means that we can drive investment to the right areas.

An additional consideration is that business service recovery priorities need to be reviewed regularly. At SWIFT we run an annual Business Impact Analysis exercise – the primary objective of which is to perform a check on our service security classification and recovery objectives to ensure these remain fit for purpose.

CHAPTER 3: OPERATIONAL RESILIENCE AND THE FPC

Question B): Would encouraging firms and FMIs to consider their contribution to the vital services that the real economy demands change the way they manage operational resilience, and if so how? What additional costs would this incur?

SWIFT response:

While there is of course huge variety amongst firms and financial market infrastructures (FMIs) active within the financial industry, it is useful that they all consider the reliance the real economy has on them, and take this into account when managing their operational resilience. At SWIFT, the design and implementation of highly resilient and secure IT infrastructure have always been part of SWIFT's global business continuity strategy. We are acutely aware of how important our services are. Some key highlights on how we have adapted our resilience and availability approach include:

- In 2007, the SWIFT board approved the commencement of SWIFT's 'Distributed Architecture' (DA) project to increase the processing capacity and resilience of the SWIFT core messaging infrastructure;

- In 2010, we reduced our service recovery time through the deployment of a new operational control centre in Asia;
- In 2014, we established a third operating centre;
- In 2016, SWIFT launched the Customer Security Programme (CSP) – a global security programme to enhance customers' operational service resilience and support customers in reinforcing the security of their SWIFT-related infrastructure. As part of this, a fully operational Security Operations Centre (SOC) was implemented.

Due to our longstanding business continuity focus, a large part of our operational costs are resilience-related – resilience of locations, systems, networks and people. Specific attention has been put into cyber resilience in recent years as we have integrated the investments for cyber resilience into our existing improvement processes. We have developed and refined our approach over the years and use a threat/risk based approach to ensure we adopt best practices while also focusing on key risks to our critical services.

CHAPTER 4: OPERATIONAL RESILIENCE OF FIRMS AND FMIS

Question C): How do boards and senior management currently prioritise their work on operational resilience?

SWIFT response:

The essential components of SWIFT's resilience are actively managed throughout the organisation – from Board level, through the SWIFT Executive and senior management, to operations.

The SWIFT Executive and Board define our vision and approve the major projects and investments in business continuity. SWIFT has long had board-level reporting on operational resilience, which is measured in terms of service availability.

Reports with insights on SWIFT's operational resilience are provided to the Board's Technology & Production, Audit & Finance and Franchise Risk Committees. This reporting structure has helped deeper embed and drive the culture of "failure is not an option" for continuous resilience improvements.

Strong governance from the Board on this issue can be evidenced through the many initiatives we have undertaken to increase our service resilience.

This leadership is vital to ensure the success of our strategy to continuously run the core business to the highest standards of resilience and security.

Additionally, risk management is deeply embedded in operational practices at SWIFT, and is underpinned by a very strong risk culture that is captured in the motto: "Failure is Not an Option" (FNAO). Three lines of defence underpin and oversee SWIFT's risk management approach: first, management, which is responsible for developing and implementing strong reliability and security frameworks; second, the risk and compliance functions, responsible for the overall risk frameworks; and third, the audit function. All of this is supported by a robust 3rd party assurance framework and through reporting by an external security audit firm, in accordance with the requirements in the applicable International Standards on Assurance Engagements.

Question D): What changes are firms and FMIs planning to make to strengthen operational resilience over the next few years? How involved are board members in the planning, implementation and embedding of any changes? What are the likely benefits and costs involved?

SWIFT response:

Ensuring operational resilience requires constant vigilance, especially given the rising threat levels and rapid technological developments. Amongst other ongoing measures, SWIFT is progressing a strategy which will allow us to further enhance our resilience capabilities.

We also continue to strengthen our identification, prevention, detection and response capabilities in light of the growing cyber arms race. We are developing our cyber recovery capabilities by:

- leveraging our already very strong and well established reliability/BCP practices to prepare us for a broader set of cyber risks;
- moving our main platform to new technology offerings;
- analysing “last resort option” to cope for extremely unlikely but severe cyber scenarios.

SWIFT Board approval is required for major operational resilience projects. If approved, the Board is kept informed about the status of the project.

CHAPTER 5: CLEAR OUTCOMES FOR OPERATIONAL RESILIENCE

Question E): What are readers’ views on the possibility of firms and FMIs being asked to set impact tolerances for their most important business services?

SWIFT response:

We believe that firms should set impact tolerances for their most important business services. At SWIFT we have already defined our ‘impact tolerance’ and review this on an ongoing basis. We would therefore not expect this to require any immediate change.

Question F): What approach and metrics do firms and FMIs currently use?

SWIFT response:

At SWIFT our business continuity and resilience approach has been integrated into the way that we do business. It is reflective of the scale and nature of our business – and is designed to meet SWIFT community needs.

Our metrics consist of many elements, including:

- continuous measurement of service availability for business services;
- over 500 business continuity exercises per year, many involving customer participation;
- internal and external audit attesting of SWIFT business continuity capability (i.e. ISAE report);
- use of Business Continuity Standard (ISO22301);
- reporting through various channels such as the Overseer report, Business Continuity items in the company's scorecard and ISAE3000 reports;
- engagement with customers to anticipate growth and capacity needs.

Question G): If these proposals would require some firms and FMIs to update part of their existing risk management framework, what would this involve?

SWIFT response:

As a critical service provider to the financial industry, operational performance is mission-critical to SWIFT. Our strong focus on operational resilience is therefore reflected in our Enterprise Risk Management (ERM) methodology.

This risk methodology includes different risk appetite levels to reflect SWIFT's diverse activities and operations. It also has a special focus on confidentiality, integrity and availability impacts (C-I-A) for risk evaluations, and a list of operational risk areas to help categorise operational risks for effective reporting. In addition we analyse extreme external risk events and their impact on our operations.

SWIFT's ERM is maintained in line with the needs of the company and industry practices. This allows the ERM methodology to stay aligned with latest operational risk trends and technology developments.
The ERM framework is overseen by the Franchise Risk Committee of the Board. Any changes to the framework require endorsement by the Executive Committee and the Board.

Question H): What are readers' views on producing an impact tolerance statement as described? What relevant operational resilience risk management documentation do firms and FMIs already produce, and how does this differ from impact tolerance statements?

SWIFT response:

We believe such an impact tolerance statement would need to be incorporated into the overall risk management approach and should closely map to the relevant risk appetite measures with regards to operational availability.

CHAPTER 6: SUPERVISORY ASSESSMENT OF OPERATIONAL RESILIENCE

Question I): What operational resilience tests or scenarios do firms and FMIs already consider and undertake for their own risk management purposes? What factors do firms and FMIs take into account when devising operational resilience tests or scenarios?

SWIFT response:

SWIFT runs more than 500 business continuity exercises on an annual basis, involving operational staff at all levels, our customers and local authorities.

Testing of recovery plans and simulation of emergency situations are a key part of Business Continuity, Crisis Management and the overall security framework at SWIFT. The disaster recovery and business continuity plans are exercised with predefined frequencies, reflecting the criticality of the services. The scheduled tests include: general service continuity tests, cyber exercises, recovery tests (including financial institutions), site takeover tests, and floor down tests.

Exercises with external participation from the banking community include, for example, the Bank of England-led continuity exercise (White Shark), or SC3 exercises.

Question J): How do boards and senior management currently gain assurance over the operational resilience of their firm or FMI?

SWIFT response:

SWIFT's senior management receives regular updates on the availability of various SWIFT services. SWIFT's Board and a number of board committees receive updates every three months on the availability of various SWIFT services. The Technology & Production Committee (TPC) covers technology and production developments. Our ISAE 3000 report provides guarantees to third parties that the right processes are in place to ensure availability.

Question K): What are readers' views on the proposed developments to the supervisory authorities' approach to operational resilience?

SWIFT response:

SWIFT is fully committed to ensuring that our oversight by the G10 Central Banks is fully aware of the Business Continuity, Crisis Management and the overall security framework at SWIFT.

Through a number of reports (mentioned above in the various answers set out above), we keep our oversight bodies informed. We believe additional supervisory reporting should always be based on existing frameworks to ensure consistency for global players like SWIFT and to avoid possible duplication of efforts.

-------------------- END OF DOCUMENT --------------------