Principles for Operational Resilience

HSBC Group response to the Basel Committee on Banking Supervision consultative document

Date: 06 November 2021

1. Executive Summary

HSBC Group welcomes the opportunity to respond to the Basel Committee on Banking Supervision (BCBS) consultative document on 'Principles for Operational Resilience'.

HSBC is one of the world's largest banking and financial services organisations. Headquartered in London, the firm operates through an international network of around 3000 offices in 65 countries and territories in Europe, Asia, the Middle East and Africa, North America and Latin America. We serve more than 39 million customers worldwide through three global businesses: Wealth and Personal Banking, Commercial Banking and Global Banking and Markets.

We are very aware that HSBC has an important role in the global financial services industry and broader global economy. We are therefore committed to continuously adapting and improving operational resilience, working actively to review and respond to the significant regulatory developments globally in this area. HSBC has already begun consolidating existing resilience-focussed measures into an Operational Resilience programme of work and has conducted pilots for the UK legal entity against the developing operational resilience requirements as we understand them.

A number of factors have led to the inclusion of the concept of "operational resilience" into specific regulatory language: accelerated digitisation (especially in the wake of the COVID-19 lockdowns), increasing use of third parties and others, including major incidents that are linked to the central regulatory priority of financial stability (such as the incidents at TSB , Maersk and Travelex). Preparing for and learning from severe incidents will build a foundation for operational resilience and ensure the safety and soundness of the global financial system. Given the multi-jurisdictional supervisory environment and the importance of operational resilience for HBSC, the financial services industry and the global economy, the BCBS consultation is a very timely and important contribution to ensuring a globally-aligned approach.

Operational resilience is an outcome. It is an organisation's ability to anticipate, prevent, adapt, respond to, recover and learn from internal or external disruption. To achieve this, there are a number of factors that we understand to be critical:

- The ability for a firm to identify aspects of their business that could have a systemic impact.
- Understanding the interconnected nature of the underlying components that are connected to systemically important services and operations, through appropriately granular mapping.
- Setting and understanding tolerances for disruption to services that are important to customers and to the market.

- Testing and monitoring the resilience of the organisation by leveraging the understanding that mapping and modelling provides, and utilising severe but plausible scenario analysis against tolerance levels.
- Visibility, at all levels of the organisation including the most senior board level, of the resilience position and the associated risks at any point in time.

We have reviewed the BCBS consultative paper against our understanding of operational resilience, gained from preceding papers and collaboration with peers across the global regulatory landscape.

2. Key points of focus

Below is a summary of the key points of focus that we propose for further review and consideration:

- Disruptions are often not just localised to a region or jurisdiction and any principles should be globally consistent. To achieve this, BCBS members should have the ability to implement an outcomes-focused approach in their jurisdictions.
- We would like to explore how best to facilitate flexibility, proportionality and a risk-based approach to supervision in order to promote financial stability. Overall, the draft principles deliver this, however differences of opinion on the mechanisms and terminology for delivering operational resilience have arisen during industry discussions (some of which BCBS have attended) and these need to be addressed.
- We need to continue global collaboration between industry and policy makers and those setting standards. It would be advantageous to all parties if a mechanism was created to facilitate this.

Therefore, we have considered the following areas in our review:

- Coordination across existing frameworks (RRP, OCIR and Operational Risk) and the requirement for additional frameworks for operational resilience.
- Scope and dimensions of the definition of "critical operations" compared to "important business services".
- How to consider impact on the customer within the context of operational resilience.
- Operational Risk is concerned with the prevention and management of known and documented risks within an organisation and may not currently consider severe but plausible operational resilience scenarios.
- How to consider the end-to-end operational view for services that may not currently form part of an organisation's risk framework approach.
- The cascade of risk through operational risk and financial mechanisms (and vice versa) that could lead to systemic failure.

We go into further detail on these themes in 3 Definitions and 4 Specific Answers to BCBS Questions, below.

3. Definitions

The specific definitions on which we are requesting additional clarity are set out below, including commentary on their application and a comparison with other regulatory language related to operational resilience, where relevant.

Critical operations:

We understand the definition of critical operations is closely linked to existing FSB regulatory direction regarding "critical functions" within a firm that are critical both to the running of the organisation and the overall stability of the market. However, we would require greater understanding of how the definition of critical operations compares with UK regulators' definition of important business services, including differences in scope. This is especially significant in relation to customer-facing functions, viewed through a "customer harm lens", where we would like to understand if this is considered out of scope for the BCBS interpretation of critical operations and operational resilience.

Risk tolerance

Greater harmonisation of the definitions of risk tolerance and impact tolerance will ensure firms can provide accurate and consistent information to regulators. Terminology regarding risk tolerance is already established and may not adequately describe systemic operational resilience scenarios.

If we understand risk tolerance as a firm's tolerance to approach or exceed risk appetite, we would like to understand if the principles outlined in the BCBS paper are inwardly focussed on an organisation, and how we should consider customers or the market as we would expect to from an operational resilience perspective.

Resilience levels (Principle 3, para 25)

Resilience levels are referred to in this section as needing to be appropriately ensured, but are not referenced elsewhere in the document. We would like to understand what this refers to and if resilience levels should be defined and articulated as part of an operational resilience approach.

4. Specific responses to the BCBS questions:

Q1. Has the Committee appropriately captured the necessary requirements of an effective Operational Resilience approach for banks? Are there any aspects that the Committee could consider further?

The requirements of an effective operational resilience approach as outlined in the BCBS CP appear to build on existing frameworks. While this will ensure that there is common language, tooling and principles to expand upon, there is a risk that overreliance on existing frameworks may not have the scope to deliver fully against operational resilience outcomes. Although language in the paper aligns with other regulatory papers that we have reviewed, in terms of similarity of general concepts and approach, some precise definitions have the potential to be misinterpreted. This could lead to inconsistent application across jurisdictions and different supervisory approaches for international firms. Our view is that there needs to be further harmonisation of understanding from the regulatory bodies, on the boundaries and intersections of operational resilience and existing frameworks, to ensure an effective outcome for all.

Q2. Do you have any comments on the individual principles and supporting commentary?

We have noted that the individual principles have been laid out comprehensively and agree that the links to existing frameworks should be enhanced in relation to operational resilience. We have included comments below regarding individual principles with requests for clarification where appropriate.

Principle 1 – Governance

As stated above in the definition section, we would need to understand what constitutes the "Operational Resilience approach": operational resilience has been referred to as an outcome of improving existing frameworks, and a requirement for a specific operational resilience framework is not clearly articulated. We note from industry discussion, especially from the large consultancy and audit firms, that operational resilience strategies and frameworks will be specifically assessed as a measure of maturity across financial services organisations and expectations in the UK are that this is a specific deliverable.

Principle 2 – Operational Risk Management

We welcome and support harmonisation of existing frameworks and a holistic approach to risk management and so would like to further clarify the use of terms such as “risk profile” and “risk tolerance” in relation to operational resilience. These terms deal with an existing probabilistic risk taxonomy and framework rather than the more deterministic “severe but plausible” operational resilience scenario.

Principle 3 – Business Continuity planning and testing

We agree business continuity exercises should cover severe but plausible scenarios and should be linked to the appropriate level of operation/service.

We would encourage further consideration of the notion that banks generally will not have a risk tolerance for disruption, but rather a risk appetite for the level of control required to mitigate expected impacts, with the assumption that controls will be effective and that when risks materialise the residual risk will be predictable and manageable.

Our current understanding is that existing terms such as “risk tolerance”, “recovery time”, and “recovery time objective” are directed at a component or taxonomy level, whereas new/revised operational resilience terms such as “impact tolerance” are required to differentiate an end-to-end service level view. We would like to understand how best to reconcile impact tolerance as set out in the UK papers with the BCBS language relating to business continuity.

Principle 4 – Mapping interconnections and interdependencies

Mapping interconnectedness and interdependencies is key to achieving an outcome of operational resilience. Greater clarity is required across the regulatory environment on terminology regarding critical operations and important business services, to ensure mapping is consistently and efficiently applied. We would additionally welcome the opportunity to explore what granularity of mapping would be most beneficial to the industry as a whole, through the collaboration mechanisms that we have suggested above.

Principle 5 – Third-party dependency management

Financial services firms are increasingly using third-parties in support of their digital agendas and the BCBS principles outline clear requirements.

One specific area to consider is that it may not in reality be possible to expect "at least equivalent Operational Resilience conditions" from third parties in all cases. It may be better to focus on improving preparedness, through provision of a set of high level principles, assessment of third parties’ capabilities against those prinicples and corresponding improvements to internal recovery procedures and back up processes.

Principle 6 – Incident Management

We recognise the principles regarding incident response are in line with current views across the industry. While sound, there is potentially a lack of specific requirements to look at managing incidents: i) with an end-to-end service view and ii) from the perspective of customer or market harm. We would require further clarification of how the BCBS principles cover a more systemic view of Operational Resilience.

Regarding use of the word “eliminated” when referring to root causes, this may not always be achievable. Consideration could be given to including the terms “appropriately remediated” or “managed” to remove the requirement to attempt to eliminate root causes that cannot be controlled, for example operational resilience scenarios involving environmental causes or one-off disasters.

Principle 7 – ICT including cyber security

No Comment.

Q3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for Operational Resilience should reflect?

. From what we have experienced and understood, our view is that COVID-19 is not a directly relatable scenario for operational resilience as we had time to prepare, critical infrastructure was not affected and there was good cooperation between banks and governments etc.

Additionally, the nature of the COVID-19 pandemic was universally impactful across the industry and market volatility was relatively short-lived and limited in terms of constricting processes and services.

One area for consideration is the understanding that, as part of any disruption, flexibility and agility is key when agreeing necessary pragmatic dispensations to policy, and that traceability of decision making is required to ensure that any temporary measures are appropriately remediated post disruption.

Q4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

Operational risk is an important contributing factor to the outcome of operational resilience, but as it is concerned primarily with the identification and mitigation of risks whereas operational resilience is more focussed on preparing the firm for dealing with the crystallisation of the risk, we feel that a full consolidation of principles on operational risk and operational resilience is not desirable.

As set out throughout this response, we believe there should be a clear distinction between the principles of operational resilience and those of operational risk. There is an advantage in continuing to keep these two themes discrete while improving commonalities and overlap with clear language and reference.

Q5. What kind of metrics does your organisation find useful for measuring Operational Resilience? What data are used to produce these metrics?

We continue to develop our existing risk and resilience metrics in line with the industry's. As outlined throughout our response to this paper however, we believe that there could be confusion between operational resilience metrics and existing operational risk metrics that will need to be appropriately mitigated through clear definitions and agreement.