Saudi Banks responds to BCBS consultative document on Principles for operational resilience

<table>
<tr><td>Bank 1</td><td>Overall, the consultation document is providing necessary guidelines for the banks. However, In our opinion the document didn’t acknowledge the fact that many banks across different geographies have created a specific and dedicated function, outside the main “Corporate Operational Risk Function (CORF)” but within the second line of defense, to look after all aspects related to the risk of business disruption and operational resilience. Different banks use different titles for this specific and dedicated function, some of which are: Business Continuity Management, Business Continuity & Crisis Management, etc

We suggest that the document should acknowledge the above fact, the absence of which may lead to confusion among various risk functions within second line of defense, gaps in implementation and inconsistencies.</td></tr>
<tr><td>Bank 2</td><td>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?

The principles provided fully cover the key lessons emerging from the impacts emanating from the COVID-19 pandemic. It is the enforcement of the principles that will play a key role in mitigating the full effects of the pandemic.

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

No further consolidation is required as we find the committee’s principles to be comprehensive and delivering adequate coverage.

Q5. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?

We have a dedicated and comprehensive BCM and Crisis management team to test and actively manage business disruption and operational resilience readiness. This is supported by internal metrics to monitor operation resilience.</td></tr>
</table>

Bank 3	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? Overall, the consultation document is providing necessary guidelines for the banks. However, The Committee could expand on how to embed an effective Operational Resilience (and Business Continuity resilience) approach within the standard operating procedures of the Bank, with an objective of having most of the Bank's functions resilient when required. Q2. Do you have any comments on the individual principles and supporting commentary? Principle 7 "ICT including cyber security" may also stress upon: a) The need to assess and ensure robust cyber security resilience in the service provider's environment. b) The need to perform third party cyber security risk assessment and mitigation of risks. Extracts from section II (7) - An evolving operational risk landscape "The Committee's guidance on operational resilience will continue to be informed by its monitoring of the impact of the Covid-19 pandemic and any lessons learned." Query: - Can the Committee elaborate on the process of incorporating Covid-19 related lessons learnt in the final guidelines on the "Principles for Operational Resilience" - Will the Committee share the Covid-19 impact result or lessons learnt with the banks before incorporating in the guidelines? 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? The Covid-19 pandemic has taught us many lessons. One of the implications of Covid-19 pandemic on work practices has been Organization-wide acceptance of Working from Home (WFH) as a "New Norm", which can be considered / reflected in this version or next revision of the "Principles for Operational Resilience".

<table>
<tr>
<td></td>
<td>
Q4. Do you see merit in further consolidation of the Committee’s relevant principles on operational risk and resilience?
Yes, in the next revision, as the Principles would be more refined, the Committee can consider consolidation (including more inter-connection with BCM).
Q4. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?
The Bank uses Key Risk Indicator (KRI) which is under the oversight of the ORM Department as a metric to measure / monitor operational resilience. The KRIs include measures such as system availability, back-up recoveries, BCM testing, cyber-attack incidents etc.
</td>
</tr>
<tr>
<td>Bank 4</td>
<td>
<table>
<tr><th>Reference</th><th>Comments</th></tr>
<tr>
<td>Page 6 – Business Continuity Planning and Testing</td>
<td>
The document should include suggestion/requirement of reaching to Tier 7 of disaster recovery to ensure business services recovery is highly automated to achieve two critical objectives:

Zero data loss.
Avoid dependency on manual/human activities to recover the business service.

</td>
</tr>
<tr>
<td>Page 6 – Mapping interconnections and interdependencies</td>
<td>
As part of mapping interconnections and interdependencies of critical applications, the document needs to elaborate on the need to identify single point of failure from system perspective and from human perspective (key man dependency).
Additionally, critical IT roles such as critical applications administrators should not be located in the same area were they are subject to the same risk for example: human virus spread (Covid-19)
</td>
</tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Page 7- Third party dependency Management</td><td>The document needs to elaborate on the need for banks to identify critical IT components/hardware and the need to have their spare part / replacement within banks premises.</td></tr></table></td></tr>
<tr><td>Bank 5</td><td>Q1. Has the Committee incorporated the appropriate revisions to the Principles? Do you have any specific comments on the revisions to the Principles and supporting paragraph?

Yes, the committee has fully incorporated the revisions to the principles. No specific comments from our side.

Q2. Are there any aspects that the Committee should consider further? We seek for guidance from the committee on the below:

1) Guidelines in respect of criteria towards measurement of the effectiveness of operational resilience in Banks.

2) Clarification on the ownership of operational resilience from governance and management perspective be assigned to Business Units being a first line of defense.

3) Guidelines / criterion on the appropriate insurance covers to mitigate impact of external events like cyber threat, pandemic & other manmade disasters.</td></tr>
<tr><td>Bank 6</td><td>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?

Answer: In the Bank’s opinion No. We feel that the following aspects may be considered.
1. Section II: Changes in operational risks are also due to changes in economic circumstances (during non-pandemic situations) and related financial instability of the banks. This should be considered as one of the causes in the evolving operational risk landscape.
2. Section III (9): To include “Cyber Security”, “Emerging Risk”, “Security of People” as one of the topics of resilience risk.</td></tr>
</table>

	3. Section V (15): To include item 2. 4. Section V (17): Add "Risk Tolerance" in the first statement as this is the maximum loss a bank is willing to take. 5. Section V (21): To include item 2. Q2: Do you have any comments on the individual principles and supporting commentary? Answer: Yes. We have stated in the above. 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? Answer: Yes. In our opinion, "Emerging Risk" is an important concept and all banks in the Kingdom should work collaboratively and discuss on Emerging Risks. This was the shortcoming in the current situation. Q4: Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience? Answer: Yes. Q5: What kind of metrics does your organisation find useful for measuring operational resilience? What data are used to produce these metrics? Answer: Metrics related to: operational resilience – conducting testing on a periodic basis, measurement of ineffective controls and monitoring the action plans, number of incidents/events and root cause analysis, Overdue action plans, Loss monitoring above risk appetite v/s actuals, IT system outages during the day or month, High risk contracts not renewed, Number of incidents involving vendors, Number of incidents of unavailability of buildings due to process failures.
Bank 7	Q4. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect? The successful implementation of the proposed principles has helped the bank to adapt effectively to the recent Covid-19 crisis. Any major

	service/operational disruption has been avoided through remote working capabilities, flexible IT infrastructure and innovative product offering, while simultaneously ensuring that cybersecurity has not been compromised. Q5. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics? A number of metrics are used at the bank level but from Operational Risk Management perspective the operational loss data and KRI Breaches are used to measure resilience. Any spike/reduction in the aforementioned metrics would indicate the level of Operational resilience from an Operational Risk perspective. Similarly, RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are among the many metrics that are being used by the Business Continuity Program.
Bank 8	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? Ans: The Committee has captured all the key elements of Operational Resilience framework inline with industry best practices and standards. Q2. Do you have any comments on the individual principles and supporting commentary? Ans: Below are few comments: **<u>Business Continuity Planning and testing</u>** As part of the testing, Banks should focus on testing the response and recovery actions rather than focusing on preventing incident from accruing. This is with an assumption that a disruption will occur and the business continuity plans should be designed with focus on how Banks would continue to deliver critical operations in those circumstances. **<u>Mapping interconnections and interdependencies</u>** As proposed, mapping could become quite complex for some Banks, especially where the people, processes, technology, facilities and information used to delivery critical operations come from across business areas, entities or different jurisdiction.

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?

Growing number of people working from home globally due to the pandemic is increasing vulnerability to cyber-attacks and increased amount of information (including customer data) travelling between institutional servers and home network is creating new challenges. There may be instances, where homeworking may not be a suitable BCP strategy for critical departments/functions dealing with sensitive data or have short recovery requirements linked to critical cut off times. Banks must ensure that adequate controls measures are in place to address the risk associated with working remotely.

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

Yes, supported

43. The Committee recognises that measuring a bank's operational resilience is in a nascent stage and further work is required to develop a reliable set of metrics that both banks and supervisors can use to assess whether resilience expectations are being met. The Committee seeks specific feedback on the following measurement-related question:

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

As part of the Governance framework each Country maintain an annual BCM activity schedule including a BCP test program. These activity schedules are tracked and monitored through an online Governance portal. On monthly basis the Operational resilience manager updates the progress of the BCM activities on the portal. A consolidated report is produced which is reviewed by the senior management governance committee on a periodic basis. This includes any exceptions and issues identified during the BCP exercises.

Completion of Business Impact Analysis (BIA), Business Continuity Plan (BCP), Crisis Management Plan (CMP), Country Strategy document,

	Regulatory Compliance tracker and BCP Exercise reports are tracked and monitored as part of the regular updates on governance portal.