Saudi Banks responds to BCBS consultative document on Revisions to the principles for the sound management of operational risk

Bank 1	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 paragraphs? Yes, all applicable comments are fully covered. There are no further comments. Q2. Are there any aspects that the Committee should consider further? No further comments with the exception of ensuring that emerging unexpected risks such as COVID 19 need to be assessed on a timely basis by the banking sector to avoid or lessen the full impacts of any such risk event occurrence.
Bank 2	In our opinion, Basel committee recognizes that sub-categories of operational risk include 'information and communication technology (ICT) risk'; 'cyber security risk'; 'non-compliance risk'; and 'business disruption risk'. However, the document didn't acknowledge the fact that many banks across different geographies have created specific and dedicated functions, outside the main "Corporate Operational Risk Function (CORF)" but within the second line of defense, to look after all aspects related to the specialist risk domains. Therefore, we suggest that the document should acknowledge the above fact and document that such risk functions should collaborate with the CORF to achieve the desired objectives of these principles and where required lead such efforts to specifically cover requirements related to their specialist risk domains.
Bank 3	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? Our Comments are as below:

	1) Clarity on what aspects of operational risk to be covered by the banks within Risk Disclosures? 2) To provide an evaluation criteria for defining materiality of risk? 3) Detailed guidelines to banks on how to implementation of ORM tools - RCSA, KRI, etc. since each bank adopt their own models making it more subjective. 4) Boundary Risk – Further clarity required on boundary risk on a market risk exposures resulting from operation risk incident from capital charge calculations perspective. 5) Internal Fraud and External Fraud are two of the operational risk event types as per Basel II and III guidelines. Clarity required in terms of functional responsibility to align fraud risk function operational risk structure from governance and fraud prevention perspectives. 6) Guidelines to get capital benefits on account of effective management of "transfer of risk to insurance"
Bank4	It is a comprehensive document. The revised version is much clearer than the previous version. The generic statements have been expanded in a way that each explains how to comply with the principles. Such clarity might impact the existing roles and responsibilities of the involved parties, ORMF and related policies coverage, and independency of Operational Risk functions. However, in our opinion, the following additions will add value to this document: Section 16: To add "Risk Capacity" as this is an important aspect in understanding what the impact will be given the current manpower / systems in use. Section 17: Add "It is recommended that staff within the three lines of defence handling risk management duties are suitably academically qualified in risk management". In our opinion qualified staff is an important aspect in understanding and implementing the operational risk framework.

	Section 34: To add a section on “Stress Testing” as it is important for bank’s to understand the reduction to their operating income in case of materializing of incidents.