Q 1. 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?

Aspects of Operational Risk resilience have been adequately covered. Data Security and Cyber Risk monitoring in a more informal atmosphere of Working From Home (WFH) / Working From Anywhere (WFA) may be covered in detail.

Q 2. Do you have comments on the individual principles and supporting commentary?

Principle 2 and Principle 3 discuss requirements for Operational Risk Management and BCP testing.

A major challenge in the Covid-19 Pandemic was the manner in which Operations in a whole unit/ geography got affected limiting access of staff to their workplaces during quarantine and declaration of lockdowns.

The risk arising from the inability of staff to access their workplaces for a long period, the human cost of such disruptions, the psychological cost of a prolonged lockdown, unsupervised working during WFH need to be articulated and ideas on how to quantify such losses can be included.

Q 3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for Operational Resilience should reflect?

There is a need to ensure Banking Service delivery as part of essential services which cannot be stopped/delayed during pandemic. Accordingly, Banks will have to move towards delivery of additional services through Digital Platform to ensure delivery of services during the Pandemic. Banks will have to ensure resilience and data security while providing the services. Due to imposition of lock-downs across a larger area, declaration of containment zones and travel restrictions, facilitating remote work and business continuity have been observed as challenges.

Q 4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

Yes. As Banks understand more about the various aspects and complexities of Operational Risk such as linkages between Human, Process, System and External aspects, there is merit in further consolidation of the Committee's relevant principles on Operational risk and Resilience.

Q 5. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?

Metric for measuring Operational Resilience

Operational resilience is defined as the ability to deliver critical operations through disruption.

In order to be considered Operationally Resilient the pre- requisites are

1. Identification of all Critical Operations
2. Ability to identify, in a timely manner, events that can trigger an Interruption to or Failure of the Critical Operations.
3. Fall back arrangements, which may be multiple, depending on the criticality of the operations, in case of disruption. This has to include plans for redeployment of resources- People and Systems
4. Testing of the sufficiency of the fall back arrangements.
5. Preparation of Impact Tolerance for failure of a Critical Operation

The following metric has been developed by us for measuring operational resilience of a Unit/ Business/Support Group in the event of an incident:

Sr No	**Scenario details post an incident (in increasing order of severity)**	**Impact on Operations**	**Resilience Level**	**Response to the incident**
1	Incident did not cause any interruption in operations	Operations continued smoothly.	Level 1	Fall back arrangements worked
2	Incident caused limited interruption in operations	a. The Bank recovered quickly without any loss/damage/sacrifice	Level 2 a	Fall back arrangements worked, but with time lag
		b. The Bank recovered with minimal loss / damage / sacrifice	Level 2 b	Fall back arrangements worked, but with some loss
		c. The Bank recovered with significant loss/damage/sacrifice	Level 2 c	Fall back arrangements worked with higher loss

3	Incident caused a great deal of interruption in operations	a. Bank was unable to come back / recover to its original process /mechanism from the incident.	Level 3 a	Fall back arrangements did not work as expected
		b. Bank had to switch to an alternate process/mechanism	Level 3 b	Fall back arrangements did not work as expected
4	Incident caused critical interruption in operations	a. Bank had to abandon the entire process /mechanism.	Level 4 a	Fall back arrangements did not work as expected
		b. There is no scope to switch to the alternate process /mechanism as it has also been critically affected.	Level 4 b	Fall back arrangements did not work as expected

Action plans for Incident Responses

1. Level 1: Periodic review and testing
2. Level 2: Review of Fallback arrangements and strengthening them
3. Level 3: Revise Fallback arrangements and test them
4. Level 4: Revisit the process understanding, strengthen the processes, prepare new fall back arrangements.

Data Used to produce these metrices

All applications which are critical to Bank's business, and any downtime of such applications could result in considerable loss of business / reputation for the Bank.