HKAB's Comments on BCBS Consultation on Principles for Operational Resilience

I. Questions from Basel Committee

Seq.	Questions	HKAB Comments
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?	The requirements captured in this consultative document will help towards building an operationally resilient bank. While definitions and approaches may differ slightly from current methodology, it is believed that the underlying approach and assumptions are appropriate. However, we would like to suggest the following for consideration: **Operational Risk Management -** we would like to suggest the Committee to outline the importance of establishing a business service view of resilience, apart from the business function approach elaborated, which could enhance the front-to-back 'line of sight' across multiple teams. **Service View -** A service resilience approach which leads to a more direct correlation between customer service and the management of resilience within the principles ensures actions are driven against client outcomes in addition to internal risk management. **Tolerance and Risk Definitions -** A more comprehensive exploration of the interaction between resilience tolerance, risk appetite, capacity and profile would enable a consistent and comparable approach across sectors. **Standardising Implementation -** Coordination across authorities globally could standardise terminology, approach, reporting, assurance and implementation timelines for operational resilience.
2.	Do you have any comments on the individual principles and supporting commentary?	We would like to suggest the following associated with selected principles:

Seq.	Questions	HKAB Comments
		Principle 1 - Governance: We suggest more guidance on the interaction between operational resilience and risk is necessary. It is believed that operational resilience helps the bank deliver a service to the customer and is not a risk type. While we recognise the appropriateness of risk management procedures in supporting the management of resilience, further guidance on how operational resilience linked to risk appetite, risk capacity and risk profile would be valuable. **Principle 5 - Third-party Dependency Management:** Managing third-parties in support of operational resilience will require coordination at a sectorial level. We suggest the consultative document make more explicit guidance across the range of regulated and non-regulated Financial Markets Infrastructures and supply chains. It is recommended that resilience considerations associated with cloud and other related remote service providers should be given specific consideration in the guidance. **Principle 6 - Incident Management:** We recommend a focus on proactive threat "hunting" as well as reactive incident management as described. This is particularly relevant for cyber incidents and the timely minimisation of impact on customer services. **Principle 7 - Information and Communication Technology (ICT) including Cyber Security:** We agree with the principle that banks should consider ICT and cyber security as fundamental to resilience. However, we would recommend that guidance associated with operational resilience methodologies take a pragmatic and balanced approach across all operational assets including ICT. Operational resilience should remain risk agnostic, whilst recognising the priority of cyber risk in security and more broadly in resilience.

Seq.	Questions	HKAB Comments
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 has been a notable increase in internal and external reporting requirements under the global pandemic. Where possible, standard and predetermined reporting by scenarios should be developed to aid incident management. On the other hand, the pandemic highlighted the need for further global consistency and coordination in the approach to operational resilience, on the value in a cross-sectoral approach to the development of global operational resilience principles, and on the need to maintain flexibility for banks to adapt to challenging circumstances and to their own respective business models. We notice that under the Covid-19 pandemic, in countries and markets with less advanced information and communication technology, the risk of operational disruptions was amplified. Typical difficulties faced including the banks' and clients' abilities and timeliness of delivering activities which require staff to be on-site, such as check processing, access to on-site vaults, receipt of documents sent via post or courier, etc. This calls for the establishment of contingency plans for banks to ensure satisfactory delivery of services. Increased Working From Home (WFH) arrangements during the pandemic raises the possibility of sustained remote working by a significant percentage of the workforce on a sustained basis during non-crisis normal operations. This would reduce concentration risk in major office buildings. Increased WFH and the associated ICT enablement brings other resilience considerations, e.g. limitation of at home printing capabilities, shortage of physical remote access tokens, understanding of remote work capabilities and supply chain dependencies of third party suppliers of banks, etc. which we suggest to the Committee to provide further guidance. We would also like to suggest the management of concentration risk (e.g. geographical and business sector concentration of client services and use of

Seq.	Questions	HKAB Comments
		third party suppliers), the potential fragility of extended global supply chains and third party suppliers during a pandemic to be considered in the guidance.
4.	Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?	We would like to suggest considering whether clarity is necessary on the interaction between the principles, methodologies and outcomes of operational risk versus operational resilience, prior to any consideration of consolidation. In addition, we would like to suggest the Committee to consider setting out additional principles on below areas: • forward-looking approach to identifying risks, threats, vulnerabilities and opportunities; • infrastructure management with suggested ways to mitigate manual intervention; and • embedding operational resilience considerations in new product design, development and approval process.
5.	What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?	We find metrics associated with operational service levels, control performance against operational risk appetite and tolerance indicators are useful for measuring operational resilience. In addition, it may be considered useful for banks to assess below aspects to understand their own resilience level and establish metrics for its measurement: 1. How do legal entities and lines of business each demonstrate that constructive efforts have been made on the bank's operational resilience?

Seq.	Questions	HKAB Comments
		2. How does the bank obtain and update its visibility on the inter-relationships and dependencies across the end-to-end components of its key business services, including inter-affiliates and third parties? 3. What are the controls protecting and sustaining key business services during disruptions, and their respective control effectiveness? 4. How does the bank determine whether and when key business services have returned to normal during disruption? Which party within the bank is responsible for endorsing this? 5. Is there adequate governance and technical capability for assessing the root cause of disruptions and identifying risks, threats and vulnerabilities faced by the bank? How does the bank demonstrate effective evaluation of such assessment by the Board and senior management?

II. Other Comments

Seq.	Relevant Extract	HKAB Comments
6.	**III Essential elements of operation resilience** 8. Operational resilience is an outcome that benefits from the effective management of operational risk. […] **IV. Definition of operation resilience** 12. […] In considering its operational resilience, a bank should take into account its overall <u>risk appetite, risk capacity and risk profile</u>. **V. Operation resilience principle**	We would like to seek clarification on whether "risk appetite, risk capacity and risk profile" as quoted under section III, IV and V only include operational risk or all types of risks of the bank. Also, we would like to suggest using the same terminology throughout the consultative document for consistency purpose, and setting out the expectation on the extent of "forward-looking operational resilience regime".

Seq.	Relevant Extract	HKAB Comments
	16. […] The practices described below, some of which reflect previously issued guidance, should not be viewed in isolation, but rather as integral parts of a bank's forward-looking operational resilience regime in line with its operational risk appetite, risk capacity and risk profile. **Governance** 17. The board of directors should review and approve the bank's operational resilience expectations considering the bank's risk appetite, risk capacity and risk profile. […]	
7.	**IV. Definition of operation resilience** 13. The term *critical operations* is based on the Joint Forum's 2006 high-level principles for business continuity. It encompasses "*critical functions*" as defined by the FSB[11] and is expanded to include activities, processes, services and their relevant support assets […] *Footnote:* [11] *FSB, Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Share Services, 2013. […]*	According to the definition set out by FSB, whether a particular operation is critical depends on the nature of the bank and its role in the financial system. This does not lend itself to a focused, significantly higher standard of operational resilience for the critically important services a bank provides. As a result it may unintentionally hinder "enhanced resilience". Hence we would like to suggest considering setting a more granular level for critical operations by also looking at what banks deliver to external entities and allow the ability to deliver a higher level of operational resilience. Furthermore, in reference to footnote 11 which quotes guidance issued by FSB, we would like to seek clarification on whether *"critical operations"* are those that are identified under the Resolution Plan and Recovery Plan of the bank?
8.	**V. Operation resilience principle** **Governance** *Principle 1: Banks should utilise their existing governance structure to establish, oversee and implement an effective operational resilience*	We would like to suggest bringing in the concept of an "end-to-end" operational resilience approach into the consultative paper so that banks evolve their existing governance structures. It is viewed that a business service view of resilience, as opposed to a business function (department /

Seq.	Relevant Extract	HKAB Comments
	approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.	process) approach, requires a front-to-back 'line of sight' across multiple teams. For example, acting as a direct custodian to give clients access to market infrastructures involves not only a "direct custody and clearing" product view, but an end-to-end view covering various aspects including sales, technology, operations, cash management, foreign exchange, sanctions screening, product control, financial, risk and regulatory reporting among others. Operational resilience requires a true end-to-end connected view.
9.	**V. Operation resilience principle** **Governance** 17. […] In formulating the bank's risk tolerance for disruption to its critical operations, the board of directors should consider a broad range of severe but plausible scenarios (eg, lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.). **Business continuity planning and testing** 24. […] Business continuity exercises should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents.	We would like to seek clarification on whether there are any differences between "the range of severe but plausible scenarios" stated under the "Governance" section and the "Business continuity planning and testing" section? If yes, please provide further elaboration. Furthermore, we would appreciate if the consultative document could provide more guidance on the expectation on the extent of such scenarios setting.

Seq.	Relevant Extract	HKAB Comments
10.	**V. Operation resilience principle** **Governance** 17. […] the board of directors should consider a broad range of severe but plausible scenarios (eg, lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.). **Third-party dependency management** 32. The *respective functions* should perform a risk assessment and due diligence before entering into arrangements including those of, but not limited to, third parties or intra-group entities, consistent with the bank's operational risk management framework, outsourcing/third-party risk management policy and operational resilience expectations. […]	We would appreciate if the consultative document could highlight the scope and definition of "operational resilience expectations".
11.	**V. Operation resilience principle** **Operational risk management** *Principle 2: Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations.*	We would like to suggest emphasising in the consultative document that operational risk and operational resilience should not be conflated, as operational resilience is broader and includes more than operational risk considerations. Other risk types such as liquidity risk, strategic risk, conduct risk, market and credit risk might also have an impact on operational resilience.
12.	**V. Operation resilience principle** **Business continuity planning and testing**	Similar to Seq.11, we would like to suggest emphasising in the consultative document that operational risk, business continuity plans ("BCP") and operational resilience should not be conflated. Achieving operational resilience, idea inception, design and build phases are all critical, as a result. While BCP focuses on planning for resilience of existing operations, we

Seq.	Relevant Extract	HKAB Comments
	Principle 3: Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.	would also like to suggest calling out new product development and approval which focuses more on the beginning stage.
13.	**V. Operation resilience principle** **Mapping interconnections and interdependencies** *Principle 4: Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations.*	Identifying critical operations could pose challenges to banks due to the following reasons: • Critical operations are too high-level and are only derived from the planning of a financial stress event, instead of operational risk. • The focus of identifying critical operations is more about going concern. • It is difficult to map end-to-end processes as some operations are internal only. Hence, we would like to seek guidance on the mapping of internal and external interconnections and interdependencies, granularity of critical operations and the mapping, as well as the expectations of banks using maps to identify vulnerabilities. We also would like to seek guidance on how banks should determine when a change is material enough to warrant a review of the mapping, in addition to annual reviews. For example, whether the resignation of a key person would warrant a review of the mapping. Furthermore, we would like to understand more on the regulatory expectation and response in a situation where a vulnerability disrupts a critical operation or business service yet was not deemed "relevant" and thus not included in the mapping.

Seq.	Relevant Extract	HKAB Comments
14.	**V. Operation resilience principle** **Third-party dependency management** *Principle 5: Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations.*	We would like to suggest the Committee to consider below recommendations: • in cases where banks consider a replacement of service provider is necessary yet no immediate substitute service providers exist, allow for a transition period for banks to find alternative solutions; • provide guidance for the standardization of information security requirements established by banks when they enter contracts with third party suppliers, which could help reduce unnecessary complexity and frustration for both the financial institutions and the third parties; and • provide further elaboration of the term "intra-group entities" to ensure alignment of the definition and interpretation of this principle across the industry.
15.	**V. Operation resilience principle** **Incident management** *Principle 6: Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.*	We fully recognize the importance of resumption of service to an institution's resiliency program, however in the cyber security context the technical capability of a firm to restore a system to operations, and the time frame for doing so, varies greatly depending on the nature of the attack and the size and complexity of the system. Rather than establishing an RTO time limit for specific systems, we recommend regulators explore an approach which focuses more broadly on resumption of service, measured by the firm's best efforts to ensure the ability to safely meet contractual and regulatory service obligations, with the firm required to sustain a good governance model that addresses all of those cyber disruptions scenarios and concerns as well as how to respond and recover from them. Regarding the timeliness and effectiveness of incident response and implementation of recovery plans, the technical capability and designated

Seq.	Relevant Extract	HKAB Comments
		time frame for execution across banks varies. It is also dependent on the nature of the incidents, and the size and complexity of impacted systems. As such, we would like to recommend the Committee to consider formulating an approach which focuses on the resumption of serves after incidents, measured by banks' best efforts to ensure compliance with contractual and regulatory service obligations. Further guideline on establishing a sound governance model, which ensures various operational disruption scenarios and concerns (especially those related to cybersecurity) are timely addressed and responded, should also be provided.
16.	**V. Operation resilience principle** **Incident management** 35. Banks should maintain an inventory of incident response and recovery, internal and third-party resources to support the bank's response and recovery capabilities. 38. […] A bank's incident management programme should manage all incidents impacting the bank, including those attributable to dependencies on, but not limited to, third parties and intra-group entities.	We would like to seek clarification on the definition of the term "inventory" and whether there is any requirement on the size and scope of inventory. Regarding incident management programme, we would like to suggest toning down the word of "all" to provide flexibility to banks, such that banks may manage a range of appropriate or assessed incidents. Otherwise, we would like to suggest the consultative document clarify the extent or scope.
17.	**V. Operation resilience principle** **ICT including cyber security** *Principle 7: Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and*	Since cyber security may not be the single threat faced by banks in an incident, compliance with multiple regulatory requirements on corresponding threats might be needed, and banks may tend to report such incident only after thorough information collection and internal assessment have been conducted. This may hinder timely incident reporting and transmission of incident information to regulators. As such, we would like to recommend the Committee to consider promoting an incident reporting

Seq.	Relevant Extract	HKAB Comments
	convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.	mechanism which allows subsequent update and adjustments to the initial reports submitted by banks.