CAPCO

# BIS HEADS IN THE WRONG DIRECTION ON OPERATIONAL RESILIENCY

The Bank for International Settlements (BIS) issued two consultation documents in August for comment by November 6:

- Revisions to the principles for the sound management of operational risk[1]
- Principles for operational resilience[2]

**For operational resiliency, Capco's perspective is BIS is headed in the wrong direction and has set a bar that is too low to drive real change.**

Below we have listed ten reasons why Capco believes the BIS consultation paper is flawed by setting both a low bar for compliance and is heading in the wrong direction without giving role clarity.

1. COVID-19 was not a major successful test of financial services resilience because:

- Extensive notice (typically ~six weeks) of impending disruption
- While there was significant market volatility, government programs and prolonged earlier periods of low-interest rates help shore up liquidity and credit markets
- Critical infrastructure was largely unaffected
- Banks worked collaboratively with governments to support customers impacted adversely by income, employment and health
- Improvements/increases in capital minimums, measuring liquidity more consistently, better credit processes and super or prime customers and collateral have all helped mitigate the current economic impacts, more will be felt in Canada and elsewhere as government programs and bank payment deferrals end and expectations of resumption of normal debt servicing flows occurs

2. While the human toll of the pandemic is truly a tragedy, operational resilience scenarios should include more rapid and severe impacts to infrastructure that impacts banks directly and indirectly **(e.g., increasingly common extreme weather events or natural disasters that disrupt power and supply chains for prolonged periods).**

3. The consultation is a missed opportunity, with many of the principles being 'motherhood and apple pie' statements and missing the elements that give the UK proposals[3] bite:

- The setting of impact tolerances based on customer impact
- Requiring boards to sign off on impact tolerances

4. In the UK, by forcing companies to define the target recovery times (impact tolerances) from the clients' perspective, their freedom is significantly limited, and they have to link recovery times to client outcomes - typically triggering a much more focused discussion.

5. The **UK Individual Accountability Regime**[4] requires individuals who are nominated as Senior Managers to take reasonable steps in performing their responsibilities. As members of legal entity boards fall into this category requiring them to sign off to the effect their firm is resilient places personal liability on them which acts to increase the oversight and ownership of operational resilience as well as the burden of proof on the executive.

6. Responsibility for operational resilience is split between operational risk, business continuity planning (BCP), 'respective functions,' and information and communication technology (ICT) without really describing how it would work in practice. Principles like mapping interconnections and interdependencies are not assigned.

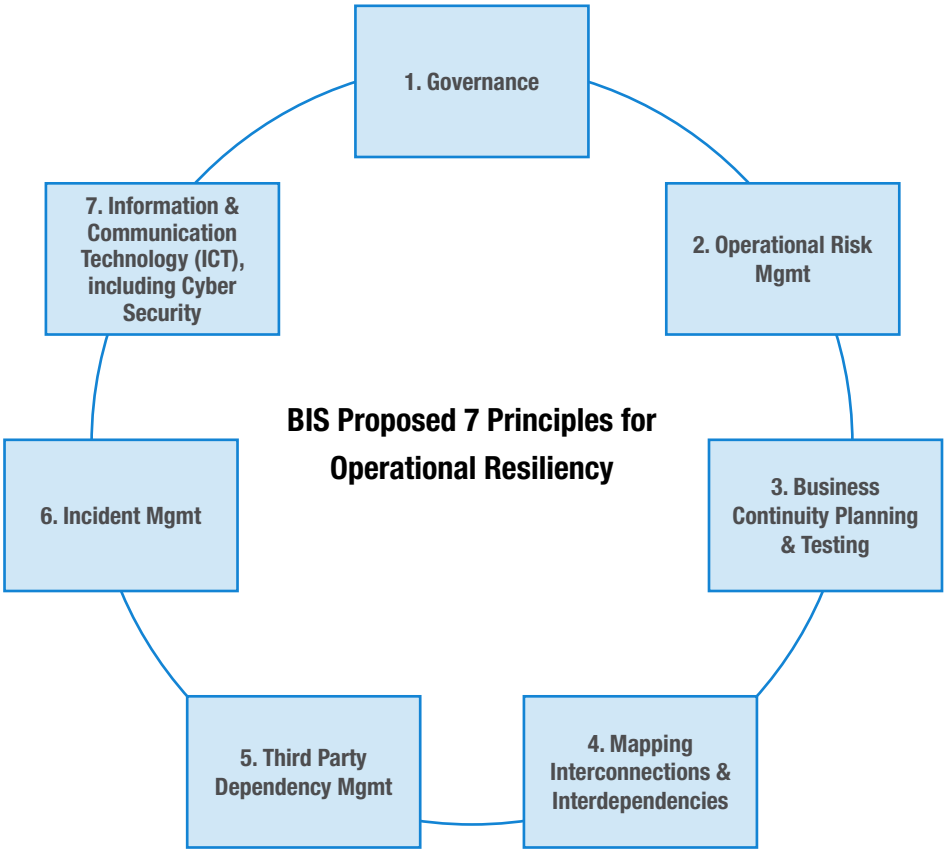
7. Operational risk falls under the risk organization while the delivery processes behind services fall under the COO, so, if anything, tasks should move from operational risk to operational resilience.

8. By framing recovery in terms of the bank's risk tolerance, it sets a lower standard that is internally focused without giving any guidance on what good looks like – so no real dimensioning. This works if regulators are genuinely happy with the current state of resilience as it will engender no real change.

9. While this is only a consultation paper, the differences between the UK regulators consultation papers published in December and this are significant with the UK rules setting a higher standard. If this gap reflects differences between regulators globally, then this will impact firms having inconsistent standards to meet depending on the legal entities used to conduct businesses.

10. For operational resilience, BIS has brought the essential elements together but not advanced the thinking deeply. For example, while third parties are included getting to fourth or fifth parties should be included along with appropriate due diligence, monitoring and reporting.

**The seven principles for operational resiliency:**



## Operational Resiliency Principles Defined[2]

1. **Governance:** Banks should utilize their existing governance structure to establish, oversee, and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events to minimize their impact on delivering critical operations through disruption.

2. **Operational Risk Management:** 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.

3. **Business Continuity Planning and Testing:** Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios to test their ability to deliver critical operations through disruption.

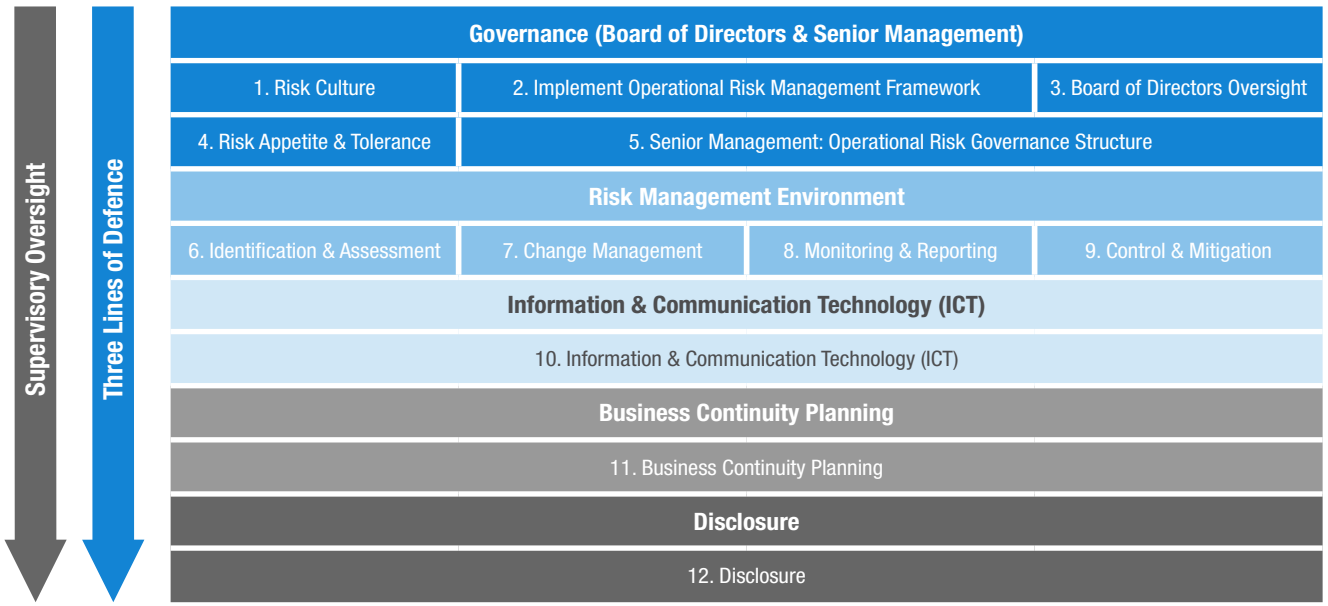
4. **Mapping Interconnections and Interdependencies:** Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations.

5. **Third-Party Dependency Management:** 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.

6. **Incident Management:** 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.

7. **Information and Communication Technology (ICT) including Cyber Security:** Banks should ensure resilient ICT including cybersecurity that is subject to protection, detection, response and recovery programs that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis to fully support and facilitate the delivery of the bank's critical operations.

**The 12 bank relevant principles for Operational Risk:**



## Operational Risk Principles Defined[1]

1. **Governance – Risk Culture:** The board of directors should take the lead in establishing a robust risk management culture, implemented by senior management. The board of directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behavior, and ensure that staff receives appropriate risk management and ethics training.

2. **Governance – Implement Operational Risk Management Framework:** Banks should develop, implement, and maintain an operational risk management framework (ORMF) that is fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.

3. **Governance – Board of Directors Oversight:** The board of directors should oversee material operational risks and the effectiveness of key controls, and ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.

4. **Governance – Risk Appetite and Tolerance:** The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume.

5. **Governance – Senior Management Operational Risk Governance Structure:** Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.

6. **Risk Management Environment – Identification and Assessment:** Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

7. **Risk Management Environment – Change Management:** Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and include continuous risk and control assessments, adequately articulated between the relevant lines of defence.

8. **Risk Management Environment – Monitoring and Reporting:** Senior management should implement a process to monitor operational risk profiles and material operational exposures regularly. Appropriate reporting mechanisms should be in place at the board of directors, senior management, and business unit levels to support proactive management of operational risk.

9. **Risk Management Environment – Control and Mitigation:** Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and proper risk mitigation and/or transfer strategies.

10. **Information and Communication Technology:** Banks should implement robust ICT governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations. ICT should be subject to appropriate risk identification, protection, detection, response and recovery programs that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis.

11. **Business Continuity Planning:** Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.

12. **Disclosure:** A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.

**Here's what Banks should do:**

- Respond to BIS by November 6, including addressing questions and providing additional comments
- Establish an operational resilience function within the accountability of the COO
- Build out a program of operational resilience following UK and BIS guidance, with linkages as needed to operational risk management
- Adopt certain leading practices
  - *Operational Resilience:*
    - Operational resiliency program has board review, approval, and ongoing oversight
    - Senior management implements with focus on key threats, vulnerabilities and critical operations, including third parties
    - Operational risk management function should work alongside other relevant functions to manage and address any risks that threaten the delivery of critical operations
    - Periodic assessments should be coordinated and manage change effectively
    - Forward-looking and flexible to accommodate potential disruptions
    - Regular business continuity testing should encompass critical operations and their interconnections and interdependencies, including third parties and intra-group entities as well as roles, decision making authority and triggers
    - Critical operations/business services are inventoried comprehensively and maintained as the organization changes including responding to external and internal events and incidents
    - Operational resilience testing includes interconnections and interdependencies mappings
    - Robust due diligence and risk assessment before contracting
    - Confirmation of third party's ability to safeguard identified critical operations to operational resilience thresholds
    - Scenarios should assess the substitutability of current third parties that provide services to the bank's critical operations, including service repatriation
    - Up to date and tested complete incident response and recovery plans, focused on defined critical operations
    - In-depth inventory of resources and capabilities that provide alternate response and recovery capacity – eliminate single points of failure
    - Third, fourth and 'nth' parties are integrated into the incident management process
    - Additional resources are available to provide an alternate response and recovery capacity
    - Root cause elimination and lessons learned include documenting those from other entities as well as third parties and intra-group entities
    - Updated effective policies and processes for critical operations asset/infrastructure inventory & assessments
    - Ongoing threat and vulnerability assessments with robust testing
    - Effective management of evolving technology in response to events and business needs covering privileged users, critical assets/information, development life cycle, critical business operations, remote assets
    - Multi-layered risk and control environment including life cycle: identify, protect, detect, respond, recover

- *Operational Risk:*
  - Clearly communicated risk culture with aligned performance management policies and practices, and effective whistleblower processes
  - Tighter alignment with enterprise risk management framework, risk appetite, risk thresholds and limits to operational risk management as well as business continuity, incidents/loss event/ICT management processes, change management
  - Further clarity regarding roles, responsibilities and interactions between and within the three lines of defense, management and the board, and their involvement with ORMF
  - ORM processes continuously evolve risks change, and are robust and reporting is timely even in periods of disruption
  - ORM focuses on both past performance but also forward-looking risk indicators to provide insights
  - ORM benchmarking to peers and use of leading/global practices and adoption of new/enhanced industry standards occurs regularly
  - Monitored training in ORM is provided throughout the bank, and supplemented for specialized roles/functions
  - ORM tools include a combination of self-assessments, event data, event management, scenario analysis, control monitoring
  - ICT risk management processes address confidentiality, integrity and availability requirements

# SOURCES


1. https://www.bis.org/bcbs/publ/d508.htm
2. https://www.bis.org/bcbs/publ/d509.htm
3. https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper
4. https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management
5. https://www.fca.org.uk/news/press-releases/new-accountability-regime-banks-and-insurers-comes-force

# AUTHOR

**John Ingold**, Partner

John.Ingold@capco.com

**Will Packard**, Managing Principal

Will.Packard@capco.com

# ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

# WORLDWIDE OFFICES

### APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

### EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

### NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

### SOUTH AMERICA
São Paulo

**WWW.CAPCO.COM**

CAPCO