BCBS PUBLICATIONS - OPERATIONAL RISK & RESILIENCE

More Relevant Than Ever (Green)

The Basel Committee on Banking Supervision, on the 31st of March 2021, released the finalised principles for operational resilience with the aim of strengthening banks' ability to absorb operational risk and to operate effectively through shock events such as pandemics, cybersecurity attacks, technology disruptions and natural disasters.

The principles encapsulate the various operational risk management frameworks and publications released by the Committee in the past two decades and provide a unified, standardised framework for banks. The document focuses on the critical elements of risk management frameworks, business continuity planning and third-party dependency management across seven categories[1] :

1. GOVERNANCE

Banks should utilise 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 in order to minimise 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 approach.

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 in order to test their ability to deliver critical operations through disruption.

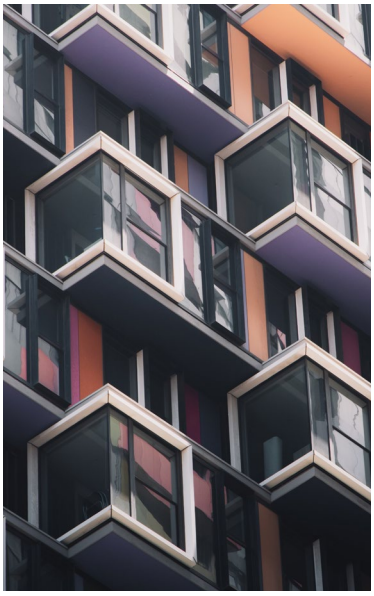
4. MAPPING OF INTERCONNECTIONS AND INTERDEPENDENCIES OF CRITICAL OPERATIONS

Once a bank has identified its critical operations, the bank should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

5. THIRD-PARTY DEPENDENCY MANAGEMENT

Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intragroup entities, for the delivery of critical operations.

1. BCBS, 'Principles for operational resilience', 2021, https://www.bis.org/bcbs/publ/d516.htm



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 appetite and tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

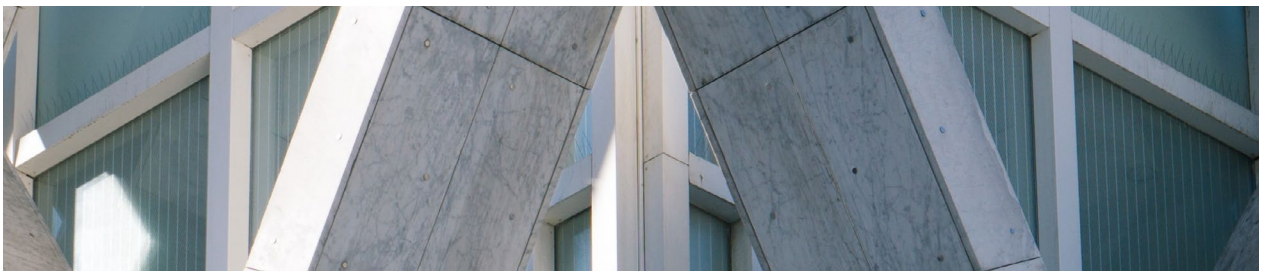
7. RESILIENT INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

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 convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

The publication follows a **principles-based approach, using proportional implementation** based on size, complexity and geographical location. While this allows for greater flexibility to ensure banks are not shoehorned into rigid requirements and specifications, the subjectivity of the principles may allow banks to inadvertently set lower standards than expected by regulators, without the clarity of a benchmark that defines resilience objectively.

Additionally, the BCBS has released the revised **principles for the sound management of operational risk (PSMOR)** to ensure banks better understand and mitigate their risk profiles. The Committee has updated the PSMOR to ensure guidance around change management and ICT, improve the overall consistency of the principles, as well as align to the **Basel III finalisation framework** for operational risk. With its effective date of 1 January 2023, the Framework will replace the use of internal models for all banks with a single simplified approach – the Standardised Measurement Approach – for estimating the capital for operational risk, using internal loss and financial statement data.

While operational resilience and risk aim to achieve different goals and are often the responsibility of different functions (COO-led vs CRO-led), they should be considered two sides of the same coin by banks and should be addressed together to mitigate both the frequency and impact of operational shock events.



BCBS's Principles for operational resilience:
https://www.bis.org/bcbs/publ/d516.htm

BCBS's Revisions to the principles for the sound management of operational risk:
https://www.bis.org/bcbs/publ/d515.htm

JOHANNESBURG

13th Floor, Greenpark Corner,
3 Lower Road, Morningside,
Sandton, South Africa

Phone: +27 (0) 11 263 5800
Fax: +27 (0) 11 263 5811
Website: www.monocle.co.za

CAPE TOWN

301 New Cumberland,
163 Beach Road, Mouille Point,
Cape Town, South Africa

Phone: +27 (0) 82 952 1415
Website: www.monocle.co.za

UNITED KINGDOM

1 Royal Exchange,
London,
EC3V 3DG, England

Phone: +44 (0) 2071 902 990
Website: www.monocle.co.uk

AMSTERDAM

Weteringschans 165 C,
1017XD Amsterdam,
Netherlands