Debate: Embedding the regulatory principles of Operational Resilience

ARMSTRONG WOLFE™

Operational Resilience: Challenges and Trends across APAC

Virtual Forum: hosted by

Maurice Evlyn-Bufton
COO
Armstrong Wolfe

Rob Scott
Former Global COO, First Sentier Investors
Armstrong Wolfe Advisor

Detailed Agenda

1. What have the other region's regulators put in place to date?
2. How have some of the APAC regulators chosen to address the topic?
3. How APAC Banks & Asset Managers are currently addressing the requirements
    - Country-by-country/regional/global approach?
    - Establish a project, or implement as part of BAU?
    - Engage an external Consultant?
    - Functional ownership?
    - Establish a dedicated business-wide Ops Resilience function, with the relevant functions reporting in to, or have an overarching framework & ongoing oversight over all the relevant functions?
    - Relevant functions being: Compliance, Risk, Business Continuity, Information Security, Supplier Mgmt.
4. What are the common themes if choosing to satisfy requirements at a regional/global level?
    - Pretty much all regulations are "principles based", which means it's ultimately up to you how you want to interpret and comply with the regulations within your business, and then the regulators will decide later whether you've complied.
    - Implementation exercise:
        - Identify "critical" operations (people/processes/systems/Suppliers)
        - Mapping interconnections and interdependencies
        - Set impact tolerances
        - Perform scenario testing
        - Implement initial improvements
        - Implement ongoing governance oversight framework
    - Governance framework.
    - Operational risk mgmt.
    - Business Continuity planning & testing.
    - Supplier dependency mgmt.
    - Incident mgmt.
    - Information and communications technology, including information security.

5. What the optimal approach might me

- All approaches can work, and not work - depends how well you execute on the chosen approach.
- Depends on your regional/global coverage.
- Depends on your ability to allocate a single owner.
- Depends on the current state of your Compliance/ Risk/Business Continuity/Supplier Mgmt/Information Security functions.

Summary of principal regulations (as at Oct 2022)

Global

- In March 2021 the Basel Committee issued Principles for Operational Resilience and then followed up some months later with updated Principles on Outsourcing.
- The Bank for International Settlements published a "Principles for operational resilience" in 2021.
- Outside of the banking sector IOSCO has published this summer a final report on the operational resilience of trading venues and market intermediaries during the COVID-19 pandemic and lessons for future disruptions.

Europe

- **UK** - New rules and guidance on operational resilience came into force on March 31, 2022. Firms within scope of the new rules must perform mapping and testing by March 31, 2025. The PRA has, so far, given soft guidance in the form of speeches setting out where it expects firms to focus on as they work towards the 2025 deadline. Further reforms in this area are on the horizon with the UK financial services authorities issuing a Discussion Paper on critical third parties.
- **European Union** - From an EU perspective, in terms of operational resilience, the regulatory spotlight has focussed over the last year or so on outsourcing and information communication technology (ICT). Significant new EU legislation is on the horizon with the Regulation on Digital Operational Resilience, otherwise known as DORA.
- **Netherlands** - The Dutch regulators are supportive of DORA. DNB has previously issued a paper reminding institutions that not only will cloud service providers be subject to EU rules under DORA but they will also be subject to national supervision under the Network and Information Security Directive which is currently being revised.
- **France** - Both the AMF and the ACPR are supportive of DORA with political agreement being reached during the French Presidency of the Council of the EU. They both have been looking at firms' cyber resilience through a wave of SPOT inspections.
- **Germany** - Germany supported the development of DORA during its Presidency of the Council of the EU. Current BaFin requirements, such as MaRisk and BAIT, already contain numerous elements of DORA. Due to the increased likelihood of a distributed denial-of-service and other cyber-attacks and the increasing digitalization of the financial markets, BaFin has announced for 2022 that it will increase its efforts to counter cyber risks and that it will conduct more dedicated IT audits at institutions and companies.
- **Luxembourg** - Luxembourg is also supportive of DORA and in June last year CSSF Director General Claude Marx acknowledged that financial services providers are becoming increasingly more dependent on the internet and information technology. In April 2022 the CSSF issued Circular 22/806 which consolidates in one place its supervisory requirements on outsourcing arrangements related to ICT.
- **Italy** - In Italy operational resilience requirements are aligned with EU regulatory provisions. More recently the Bank of Italy has focussed on cyber security and has adopted a series of supervisory actions to closely monitor the ability of supervised entities to promptly deal with cyber events and crisis.

North America

- **United States** - Operational resilience remains a priority for regulators as illustrated by the most recent Exam Priorities issued by the SEC Division of Examinations. On the banking side, efforts were made in October last year by U.S banking regulators to consolidate materials into a single paper, Sound Practices to Strengthen Operational Resilience. Noting the importance of cyber resilience to operational resilience the paper contained an annex on managing cyber risk and the SEC has taken this a step forward by issuing a comprehensive set of proposed reforms to improve cyber security risk management.
- **Canada** - OFSI is expected to consult on proposals revising its consolidated guidance for operational risk management for federally regulated financial institutions (FRFIs). OFSI has also issued a consultation on revisions to its guidelines on third party risk management and issued guidelines for how FRFIs should manage technology and cyber risks.

Middle East

- **United Arab Emirates** (DIFC) - The DFSA is maintaining its strong supervisory focus on the operational resilience of firms and this includes its ongoing focus on cyber-security risk.

Africa

- **South Africa** - With the issue of Directive 2021/10 (D2021/10), the following principles, as set out by the Basel Committee, are applicable to the banking industry in South Africa i.e.: governance; operational risk management; business continuity planning and testing; mapping of interconnections and interdependencies of critical operations; third-party dependency management; incident management; and resilient information and communication technology, including cyber security. All banks must comply with the respective requirements specified in D10/2021 by June 2023.

APAC

- **Australia**
  - **ASIC** - Jun 2022 - Issued new market integrity rules intended to promote technological and operational resilience of securities and futures markets operators and participants - effective Mar 2023.
  - **APRA** - Jul 2022 - Released a consultation paper on a new prudential standard designed to strengthen the management of operational risks in the banking, insurance and superannuation industries. Consultation to be conducted over 2023 - effective in 2024.

Hong Kong

- **HKMA** - May 2022 - Issued a new Supervisory Policy Manual (SPM) module on operational resilience together with a revised version of the SPM module on business continuity planning. HKMA is expecting authorised firms to develop operational resilience frameworks, determine the timeline by which it will become operationally resilient by May 2023, then become resilient no later than May 2026.
- **SFC** - Feb/Mar 2022 - Published reminders to FIs on their BCP standards.
  - Effective governance framework
  - Effective Op Risk Mgmt
  - Effective information and communications systems
  - Identify key third party dependencies, evaluate risks, manage identified risks

Reference/Sources

https://www.nortonrosefulbright.com/en-hk/knowledge/publications/3215deb7/operational-resilience-regulation-around-the-world

https://www.bis.org/fsi/fsisummaries/op_resilience.htm#:~:text=The%20POR%20define%20operational%20resilience,from%20threats%20and%20potential%20failures

https://www.apra.gov.au/news-and-publications/apra-consults-on-new-prudential-standard-to-strengthen-operational-resilience

https://www.pwc.com.au/assurance/operational-resilience.html

https://www.thebci.org/news/business-continuity-vs-operational-resilience.html

https://resourcehub.bakermckenzie.com/en/resources/fsr-momentum-monitor/APAC/peoples-republic-of-china/topics/operational-risks-and-resilience

https://kpmg.com/jp/en/home/insights/2023/02/fs-operational-resilience.html

Singapore

- MAS
  - **June 2022** - Revised their Business Continuity Guidelines - effective June 2023.
    - Identify critical business services
    - Establish service RTOs
    - Map interdependencies
    - Annual review
    - Review overall framework, and each business service every 3 years
    - Annual senior manager attestations
  - **Aug 2022** - Issued an information paper regarding Operational Risk Mgmt, focusing on Third party Risk Mgmt. MAS expects banks to benchmark their practices against the information paper. It also encourages non-bank financial institutions to adopt the good practices in the information paper where relevant.

China

- **CSRC** - Apr 2022 - Issued a consultation paper regarding its intention to adopt regulations to establish a sound regulatory system for cybersecurity in the securities and futures industry.

Japan

- **JFSA** - Dec 2022 - released a discussion paper titled “Basic Approach to Ensuring Operational Resilience”, which reflects recent market developments and is aligned with the latest approaches of global financial authorities.
  - Identify critical operations
  - Set tolerance for disruption
  - Map interconnections and secure necessary resources
  - Verify appropriateness and taking additional measures.

Contact us

Maurice Evlyn-Bufton
CEO, Armstrong Wolfe
maurice.evlyn-bufton@armstrongwolfe.com

Gwen Wilcox
COO, Armstrong Wolfe
g.wilcox@armstrongwolfe.com

Find us on LinkedIn: Armstrong Wolfe

Find us on LinkedIn: Women in the COO Community

ARMSTRONG WOLFE™