



Compliance to Growth:

Navigating the BMA's New Operational Resilience & Outsourcing Regulations

Financial markets across the globe are becoming more interconnected than ever, driven by rapid advancements in technology, and strategic business partnerships. As a result, customer expectations have shifted—today's consumers demand real-time, seamless access to financial services, with zero tolerance for disruptions. However, ensuring continuous service delivery is no longer just an internal challenge; it extends beyond an organization's walls to third-party vendors, and outsourcing partners. Financial institutions must now navigate complex interdependencies, addressing not only operational risks but also regulatory concerns and building a culture of operational resilience.

In response to these growing complexities, the Bermuda Monetary Authority (BMA) has introduced new operational resilience and outsourcing regulations to help the financial sector withstand disruptions and manage third-party risks more effectively. Compliance is no longer just a regulatory obligation but a strategic necessity for long-term stability and growth. Below is an overview of the major shifts introduced by this proposal and their impact on organizations.

Operational Resilience

The BMA has shifted away its focus from operational risk and has highlighted the critical importance of operational resilience which should be embedded throughout the organization at all-levels rather than an add-on program to tackle today's complex challenges. The following has led to the key shifts in how financial institutions must approach operational resilience:

- Institutions must identify Important Business Services (IBS), map their interdependencies, and establish response plans with defined impact tolerance limits to mitigate disruptions. They must ensure the continuous delivery of IBS, regardless of third-party dependencies, by implementing robust resilience measures.
- Boards are now explicitly responsible for overseeing resilience and outsourcing risks. The annual self-assessment to demonstrate compliance with the Code must be approved by the Board and be readily available to the BMA upon request. The Board and Management must oversee and review Business Continuity Plans (BCP), Disaster Recovery Plans (DRP) to ensure their effectiveness and be responsible for approving resilience plans and the risk appetite.
- Unlike traditional business continuity plans (BCPs), resilience now requires stress testing under real-world scenarios. Firms must ensure they can recover from major disruptions within defined impact tolerances which goes beyond IT systems.

Outsourcing Management

Financial institutions are increasingly outsourcing critical functions, heightening their dependence on third-party providers and exposing them to operational disruptions. In response, the BMA has introduced stricter outsourcing standards focused on governance, risk assessment, transparency, and accountability. The key changes are outlined below:

- Institutions must manage third-party concentration risk. The board must oversee and approve the risk management process including vendor evaluation and monitoring.
- All institutions must notify the BMA before outsourcing a critical activity and may proceed if no objection is received within 30 days. Any significant changes to previously approved outsourcing arrangements will also be considered a material change in business, requiring institutions to comply with statutory notification requirements.
- Institutions must establish comprehensive communication plans with IBS partners to mitigate disruptions. These plans should clearly outline escalation protocols, key decision-makers, and effective stakeholder communication methods.
- Note that the proportionality principle is still relevant and compliance with the regulations are based on the institutions unique risk profile, considering factors such as size, complexity, and operations.

Compliance Deadlines

The final version of the code is going to be introduced in 2025 after a 60-day consultation period with the relevant entities, which includes (re)insurance entities. Comments are to be received by the BMA before 14 March 2025.

All the relevant entities licensed under the Bank and Deposit Companies Act (BDCA) are required to adhere to the requirements by **31 March 2026**. All other subject entities (namely insurers registered as Class 3A, 3B, 4, C, D, E, IIGB, and IILT) will be required to adhere to the new requirements by **31 March 2028**.

The Role of Internal Audit

Internal Audit (IA) should play a key role in service mapping, including identifying IBSSs, and assessing evolving third-party relationships. IA should ensure effective reporting surrounding outsourcing to the Board and subcommittees while evaluating whether outsourcing models support long-term resilience. Additionally, IA should conduct compliance assessments against revised guidelines and provide timely feedback to help organizations meet regulatory deadlines. As organizations prepare for the compliance deadlines, the question is no longer if they should enhance their resilience frameworks, but how they can do so efficiently and strategically.

How we can help

Deloitte has extensive knowledge of the Bermuda regulatory framework and continues to provide training and guidance to Bermuda licensed insurers on regulatory compliance. We have a strong working relationship with the BMA and Bermuda licensed insurers to stay abreast of any regulatory changes or innovations in industry practices so that we can share our insights with our clients.

We have also supported many insurers in conducting code gap assessments, building operational resilience frameworks and drafting outsourcing policies. Our expertise extends further to include Business Continuity and Disaster Recovery planning, providing comprehensive support for insurers operating in the Bermuda market. We provide deep industry insights to help you navigate complex regulations and strengthen your risk management framework, ensuring agility and long-term success in Bermuda's evolving financial landscape.

Our team



Helder Carreiro

Partner, Risk Advisory

+1 441 299 1308

heldar.carreiro@deloitte.com



Clayton Chuah

Director, Consulting

+1 441 299 1372

clayton.chuah@deloitte.com



Rudy Sawhney

Senior Consultant, Risk Advisory

+1 441 299 1334

rusawhney@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. Deloitte Ltd. is an affiliate of DCB Holding Ltd., a member firm of Deloitte Touche Tohmatsu Limited. This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.