BERMUDA MONETARY AUTHORITY

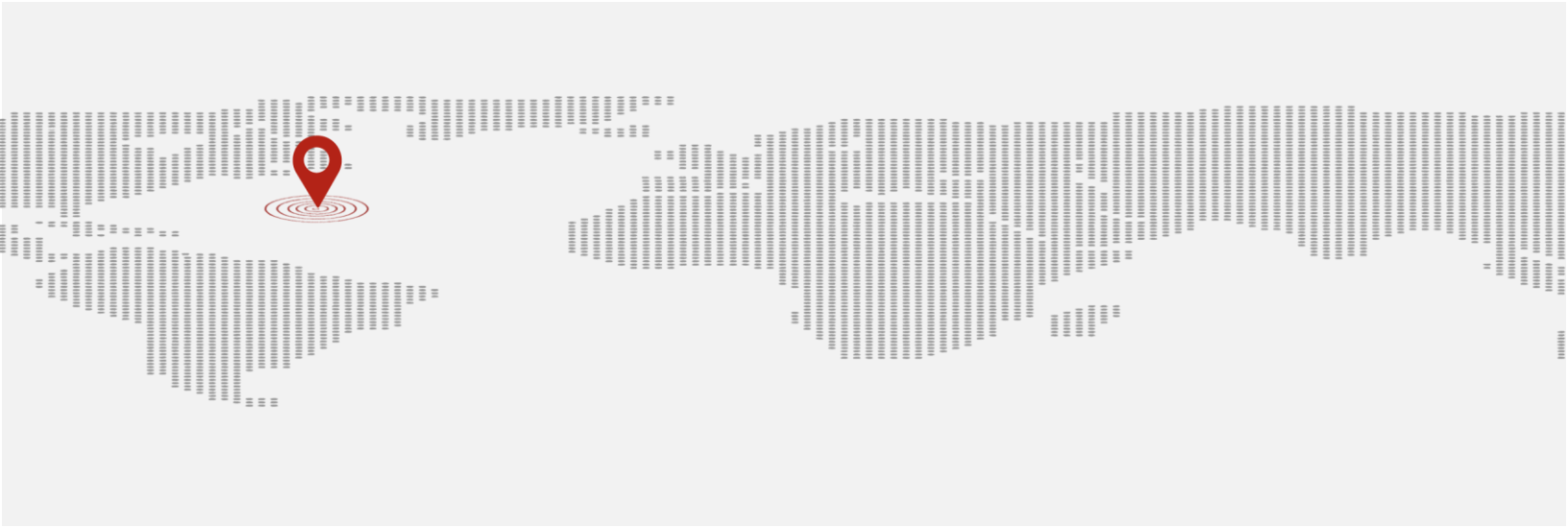
Tuesday, 14 January, 2025

CONSULTATION PAPER

OPERATIONAL RESILIENCE AND OUTSOURCING CODE

CORPORATE SERVICE PROVIDERS, TRUST BUSINESSES, MONEY SERVICE BUSINESSES, INVESTMENT BUSINESSES, FUND ADMINISTRATION PROVIDER BUSINESSES, BANKS AND DEPOSIT COMPANIES, DIGITAL ASSET BUSINESSES, COMMERCIAL INSURERS, IIGB AND IILT INSURERS, INSURANCE MANAGERS, INSURANCE BROKERS, INSURANCE MARKETPLACE PROVIDERS AND AGENTS

Comments to be received by 14 March 2025



Contents

I. INTRODUCTION

1. The purpose of this Consultation Paper (CP) is to gather feedback from stakeholders on the Bermuda Monetary Authority's (Authority or BMA) proposed Operational Resilience (Op Res) standards for financial institutions. These standards are designed to strengthen the sectors' capacity to prevent, adapt and manage, and recover and learn from operational disruptions, whether they arise within the organisation or from third-party service providers engaged by the organisation. The aim is to ensure that critical services for customers can continue operating without delays or interruptions.

2. The proposed standards are detailed in the *Operational Resilience and Outsourcing Code* (Code), supported by the *Operational Resilience and Outsourcing Guidance Notes*. Both documents are included with this CP for public review and feedback.

3. The BMA intends to introduce a final version of this Code during 2025 after a 60-day consultation period.

4. Impacted financial institutions will be given a transitional period before being required to adhere to the Code's requirements. Relevant Entities (REs) will be required to adhere to its requirements by 31 March 2028. The only exception to this will be for REs licensed under the Banks and Deposit Companies Act (BDCA), which are required to adhere to the requirements by 31 March 2026.

5. The variation in transitional periods is based on the critical role the local banking industry plays in the overall financial sector and its extensive customer base, both retail and commercial. It is important to note that any existing legislation or guidance will remain applicable until the Code becomes effective.

6. Industry and other stakeholders are invited to provide feedback on the proposals outlined in this paper and its attachments by emailing their comments to policy@bma.bm by the close of business on 14 March 2025.

II. BACKGROUND

7. Financial service providers are becoming increasingly interconnected across global networks as they cater to a diverse and expansive customer base via innovative technologies. This interconnectedness reflects the growing integration of financial markets and services worldwide, where transactions and operations often span multiple countries and time zones. As a result, the delivery of financial services has evolved into a continuous, non-stop operation—available 24 hours a day, 365 days a year.

8. Customers expect and rely on real-time access to financial services, whether trading globally, transferring funds or using online banking. This constant demand underscores the critical importance of Op Res, as even brief disruptions can have significant impacts, undermining consumer trust and potentially threatening financial stability.

9. Op Res is designed for organisations to prevent, adapt and respond to, and recover and learn from operational disruptions to ensure the continuity of critical services despite disruptive events. It also promotes a 'resilience by design' mentality within organisations, where resilience is embedded throughout all operational levels rather than being viewed as an add-on.

10. Op Res should not be mistaken for operational risk. Operational risk involves the potential for loss due to failures in internal processes, people, systems, or external events such as fraud or natural disasters. It focuses on identifying, assessing, and managing risks that could disrupt normal business operations. Conversely, Op Res emphasises an organisation's ability to anticipate, withstand, recover from, and adapt to disruptions. In summary, operational risk management aims to prevent or mitigate risk. Op Res seeks to ensure that financial service providers can continue delivering critical services effectively, even in the face of such risks.

11. Additionally, financial regulators have observed that traditional operational risk management approaches are inadequate for today's complex challenges. The Code sets clear expectations and standards to be met by financial institutions, enabling them to protect critical operations, maintain customer trust, and contribute to the stability of the financial system.

12. The BMA's proposed Code is driven by key factors, including the rising frequency and severity of operational disruptions, which highlight the need for financial institutions to enhance their ability to anticipate, withstand, recover from, and adapt to such events.

13. The Code also addresses the growing dependence on third-party service providers, which can introduce additional vulnerabilities and complexity into financial institutions' operational frameworks. By setting standards for managing dependencies on third parties, the Code aims to help licensed financial service providers mitigate the risks associated with outsourcing. It ensures that providers remain accountable for the resilience of their operations, no matter where or how their operations are conducted.

III. KEY PROPOSALS

A. SCOPE

14. The Code is intended to apply to the BMA-regulated financial institutions, which will collectively be referred to as Relevant Entities (REs), and the eight legislative acts (together referred to as the 'Acts') listed below:

    a. Commercial Insurers registered as Class 3A, 3B, 4, C, D and E pursuant to sections 4DA, 4DB, 4E, 4ED, 4EE and 4EF of the Insurance Act 1978 respectively;

    b. Insurers registered as Class IIGB and IILT pursuant to sections 4EI and 4EJ of the Insurance Act 1978, respectively;

c. Persons registered as Insurance Managers, Brokers, Insurance Marketplace Providers and Agents in accordance with the Insurance Act 1978;

d. Digital Assets Businesses (DABs) issued a Class F license pursuant to section 12(3)(a) of the Digital Asset Business Act 2018;

e. Persons licensed to carry on a deposit-taking business in accordance with the Banks and Deposit Companies Act 1999;

f. Persons licensed to carry on trust business in accordance with the Trust Business Act 2001;

g. Persons licensed to carry on corporate service provider business in accordance with the Corporate Service Provider Business Act 2012;

h. Persons licensed to carry on money service business in accordance with the Money Service Business Act 2016;

i. Investment Businesses issued a standard licence pursuant to section 16(1B)(a) of the Investment Business Act 2003; and

j. Persons licensed to carry on fund administration provider business in accordance with the Fund Administration Provider Business Act 2019.

15. The Code will not apply to any REs licensed under a regulatory sandbox or test licence by any designation.

16. The scope of the REs included in the Code was determined based on two key factors: the systemic importance of their industries to the local financial market and the nature of their customer-facing operations within their respective sectors.

B. PROPORTIONALITY

17. The Authority acknowledges that REs exhibit diverse risk profiles due to their operational differences. Therefore, it will evaluate an RE's compliance with the minimum licensing criteria for prudent business conduct by assessing whether the RE has adhered to the Code in a way that is commensurate with the nature, size, complexity, and overall risk profile of its business operations. These factors will be evaluated in a holistic manner, rather than in isolation.

18. The proportionality principle applies to all requirements of the Code.

C. IMPORTANT BUSINESS SERVICES

19. To ensure Op Res is achieved, REs must identify their Important Business Services (IBS), which, if disrupted, could cause significant harm to consumers, stakeholders or the financial stability of the jurisdiction, beyond mere inconvenience. This identification process should consider various factors, including services provided by related and third parties. The board and senior management are responsible for ensuring the identified IBS align with the RE's size, nature, customer base and complexity. REs must regularly review and update their IBS to ensure they remain relevant and effective in meeting operational needs. REs should ensure the resilience of an IBS, regardless of third-party involvement.

20. An RE must identify and document all resources, people, processes, IT systems, data and facilities essential for delivering important business services. The identification and documentation of all resources should be detailed enough to support the RE's testing, vulnerability remediation, prioritisation and investment in resilience. The Authority's Cyber Codes of Conduct include requirements for IT vendors. However, the Op Res Code extends this scope to non-IT-related vendors. Resources should be mapped, whether internal, intra-group, or third-party, with oversight and resilience assurance required. The mapping exercise should be reviewed by senior management, approved by the board, and updated annually, especially after significant changes in business, services, or resources occur.

D. OUTSOURCING

21. REs' growing reliance on third-party service providers for the management and delivery of critical activities has amplified Op Res concerns. With REs increasingly outsourcing essential functions, they are becoming more dependent on these external partners for the continuity and reliability of their services. This dependency introduces several risks, such as potential service disruptions, security vulnerabilities and challenges in maintaining consistent delivery of critical activities.

22. The Code establishes standards for managing outsourcing, including governance, risk assessment, transparency and accountability. An RE's board must oversee and approve a risk management process, including adequate vendor evaluation and monitoring. REs are required to have a board-approved policy for assessing and reviewing service providers and must conduct risk evaluations before entering into outsourcing arrangements. They must also manage concentration risks related to key service providers and subcontractors.

23. Proposed amendments to the relevant primary Acts will require REs to adhere to their obligations related to material changes in business, including the proposed outsourcing of a critical activity. The BMA proposes a requirement for REs to inform the Authority about such outsourcing arrangements before putting them into effect, and the RE may proceed if a 'no objection' notification is received within 30 days following receipt of the original notification. If the Authority contemplates raising an objection, it will serve a preliminary notice that grants the RE 28 days to submit further information. These responses hold the

potential to shape the Authority's final decision. In case of any objections, the Authority will formally convey the reasons in writing

24. Further to the previous paragraph, where an RE has previously received approval for a material outsourcing arrangement that subsequently undergoes substantial alterations from the circumstances under which it was initially approved, such an alteration will also constitute a 'material change in business'. The RE will similarly need to comply with the relevant statutory notification requirements.

E. GOVERNANCE

25. The board and senior management of an RE are crucial in ensuring Op Res by setting strategic direction, establishing governance frameworks, and regularly reviewing and approving resilience plans and risk appetite. Their responsibilities include oversight of outsourcing arrangements, ensuring alignment with strategic objectives and regulatory requirements, and allocating sufficient resources to bolster the organisation's ability to withstand and recover from disruptions. Additionally, it is the BMA's expectation that the board and senior management of an RE oversee and review the Business Continuity Plans (BCPs) and the Disaster Recovery Plans (DRPs) to maintain their effectiveness. Regular reporting on Op Res measures should be integrated into the RE's risk management framework to enable real-time monitoring of potential disruptions.

F. SELF-ASSESSMENTS AND RETURNS

26. The BMA is proposing to amend the applicable primary Acts, requiring REs to complete an annual self-assessment to demonstrate compliance with the Code requirements. This self-assessment would need to be approved by the board, retained for a minimum of five years from the date of completion and be readily available to the BMA upon request. The proposed Code outlines the minimum areas that the self-assessment should cover, including the methodology employed, identification of IBS, impact tolerance metrics, disruptive scenarios under consideration, outcomes from testing and any enhancements made to strengthen resilience.

G. TESTING

27. For Op Res, it is assumed that disruption through severe but plausible scenarios will occur. The focus of Op Res is on maintaining service continuity during disruptions rather than assessing their likelihood. Testing of resilience should ensure that IBS can withstand severe but plausible disruptions, with test plans reviewed annually or after significant changes. Even when outsourced, it is the BMA's expectation that REs will validate test results and maintain oversight of third-party arrangements, including intra-group arrangements.

28. It is the Authority's expectation that identified vulnerabilities are addressed promptly. Remedial actions should be comprehensive, taking into consideration broader implications for the financial sector.

H. COMMUNICATION PLANS

29. REs should create a communication strategy to manage and mitigate disruptions, with tailored internal and external plans for severe but plausible scenarios impacting their IBS. These plans should include clear escalation paths, the decision-makers and the methods for timely stakeholder updates, including indirect channels such as website notifications. Regular testing, including key vendor participation, is crucial to ensure readiness and effectiveness during disruption.

Bermuda Monetary Authority

BMA House

43 Victoria Street

Hamilton HM 12

Bermuda

Tel: (441) 295 5278

Fax: (441) 292 7471

Website: https://www.bma.bm

BERMUDA MONETARY AUTHORITY

OPERATIONAL RESILIENCE AND OUTSOURCING CODE

CORPORATE SERVICE PROVIDERS, TRUST BUSINESSES, MONEY SERVICE BUSINESSES, INVESTMENT BUSINESSES, FUND ADMINISTRATION PROVIDER BUSINESSES, BANKS AND DEPOSIT COMPANIES, DIGITAL ASSET BUSINESSES, COMMERCIAL INSURERS, IIGB AND IILT INSURERS, INSURANCE MANAGERS, INSURANCE BROKERS, INSURANCE MARKETPLACE PROVIDERS AND AGENTS

[January 2025]

Table of Contents

I. Legislative Basis and Scope of Code

1. This Operational Resilience and Outsourcing Code (Code) is issued by the Bermuda Monetary Authority (Authority or BMA) in accordance with the following sections of the named legislative acts below (Acts):

    a. **Banks and Deposit Companies** – section 8A, Banks and Deposit Companies Act 1999 (BDCA);
    b. **Corporate Service Providers** – section 7, Corporate Service Provider Business Act 2012 (CSPA);
    c. **Trust Businesses** – section 7, Trusts (Regulation of Trust Business) Act 2001 (TBA);
    d. **Money Service Businesses** – section 7, Money Service Business Act 2016 (MSBA);
    e. **Investment Businesses**– section 10, Investment Business Act 2003 (IBA);
    f. **Fund Administration Providers** – section 7, Fund Administration Provider Business Act 2019 (FAPA);
    g. **Digital Asset Businesses** – section 6, Digital Asset Business Act 2018 (DABA); and
    h. **Insurance** – section 2BA, Insurance Act 1978 (IA).

2. Failure to adhere to the requirements set out in this Code will be considered by the Authority when determining whether a Relevant Entity (RE) is fulfilling its obligation to conduct its business prudently. In this Code, a Relevant Entity is an entity licenced by the Authority under the relevant acts above. This includes, among other matters, ensuring that it has implemented adequate systems of control of its business and records that are appropriate to the nature, scale, and complexity of its business risk profile, as detailed under the relevant sectoral Acts as follows:

    a. **BDCA** - Second Schedule, paragraph 4(7) (10);
    b. **CSPA** – First Schedule, paragraph 3(3) 3 (2);
    c. **TBA** - First Schedule, paragraph 5 (4);
    d. **MSBA** – First Schedule, paragraph 2 (4));
    e. **IBA** - Second Schedule, paragraph 5 (6);
    f. **FAPA** – First Schedule, paragraph 2(4) ;
    g. **DABA** – First Schedule, paragraph 2(4); and
    h. **IA** – Schedule, paragraph 4(3).

3. The Code applies to the following REs:

    a. Commercial Insurers registered as Class 3A, 3B, 4, C, D and E pursuant to sections 4DA, 4DB, 4E, 4ED, 4EE, and 4EF, of the Insurance Act 1978, respectively;

    b. Insurers registered as Class IIGB and IILT pursuant to sections 4EI and 4EJ of the Insurance Act 1978, respectively;

    c. Insurance Managers, Insurance Brokers, Insurance Marketplace Providers and Agents;

d. Digital Assets Businesses issued a Class F license pursuant to section 12(3)(a) of the Digital Asset Business Act 2018;

e. Persons licensed to carry on a deposit-taking business in accordance with the BDCA ("Banks and Deposit Companies Act");

f. Persons licensed to carry on Trust Business in accordance with the Trusts (Regulation of Trust Business) Act 2001;

g. Persons licensed to carry on Corporate Service Provider business in accordance with the CSPA ("Corporate Service Providers Act");

h. Persons licensed to carry on Money Service Business in accordance with the MSBA ("Money Service Businesses Act");

i. Investment Businesses issued a standard license pursuant to section 16(1B)(a) of the Investment Business Act 2003; and

j. Persons licensed to carry on Fund Administration Provider business in accordance with the FAPA ("Fund Administrator Providers Act").

The Code will not apply to any RE licensed under a regulatory sandbox or test license by any designation.

4. The Code should be read in conjunction with the accompanying *Operational Resilience and Outsourcing Guidance Notes* (GN), which clarifies and provides detailed explanations of the Code's various requirements.

5. This Code and its supportive guidance supersede the Authority's *Outsourcing Guidance Notes*, which were issued in June 2019 and apply to Banks, Deposit Companies, the Bermuda Stock Exchange, Corporate Service Providers, Trust Companies, Money Service Businesses, Investment Businesses, and Fund Administrators.

II. Objectives

6. The primary objective of the Code is to bolster the resilience of REs and the broader financial sectors in Bermuda against operational disruptions. This objective extends beyond mere recovery from disruptions; it encompasses proactive measures to assist in preventing such disruptions and ensure the continuity of critical business services for customers. REs are expected to implement robust systems and processes that can withstand operational shocks, thereby maintaining the stability and integrity of their services. This not only aids

in safeguarding the individual REs but also contributes to the overall resilience of Bermuda's financial services sector.

7. The Code is designed to foster a culture of resilience within REs by establishing requirements for responsibilities, standards, procedures, and principles concerning operational resilience (Op Res). This aids the BMA in incorporating Op Res into its prudential framework. The Code serves as a foundation for the BMA to evaluate the Op Res of REs and mandate improvements when deemed necessary. This approach ensures that resilience is not an afterthought but a fundamental aspect of RE's operational strategy and culture.

8. All REs are mandated to adhere to, adopt, and implement key operational resilience principles, which include:

   - **Resilience by design:** rather than retrofitting, instead build resilience into the design of business processes, customer-facing services and supporting resources at inception

   - **Operate in a resilient manner:** ensure the capability to absorb operational shocks and continue delivering critical services, even during disruptions

   - **Continuous improvement**: regularly evaluate and enhance operational resilience through ongoing learning, stress testing, and feedback mechanisms, keeping the organisation agile and responsive to emerging risks

9. The Code is not exhaustive. REs must implement adequate governance and sufficient Op Res programmes to ensure Op Res is implemented in a timely and effective manner. REs are required to show that there has been board review, approval, and continued governance of Op Res to ensure policies, procedures, and controls concerning operational resilience remain relevant.

III. Proportionality Principle

10. The BMA appreciates that REs have varying risk profiles based on their businesses' nature, scale and complexity. REs with higher risk profiles, due to their scale or business model complexity, require more comprehensive governance and risk management frameworks to conduct business in a sound and prudent manner.

11. Accordingly, the Authority will assess the RE's compliance with the minimum criteria for licensing requirements by determining if it has adhered to the Code in a proportionate manner relative to the nature, scale and complexity of its business operations. These elements are considered collectively rather than individually (e.g., an RE could be relatively small in scale but provide essential or important business services); therefore, it is required to ensure a high level of operational resilience. In defining these elements:

- **Nature** defines the relationship between the client entity and the undertaking or characteristics of the service provided

- **Scale** refers to the volume of business conducted or the size of the balance sheet in conjunction with materiality considerations

- **Complexity** includes organisational structures and ease of information transmission

- **Overall risk profile** includes the extent to which the services provided by the RE have systemic significance and the extent to which disruption to services provided by the RE has implications for customers, counterparties, and Bermuda's financial stability

12. In assessing the existence of prudent business conduct, the Authority regards both its prudential objectives and the appropriateness of each requirement specified in the Code. The proportionality principle described above applies to all requirements of the Code, regardless of whether the principle is expressed in it.

IV. Operational Resilience Background

13. REs are increasingly interconnected in the financial world to provide financial services to retail consumers or business to business (both hereafter referred to as 'consumers'). In addition, the delivery of financial services is 'always on': 24 hours a day, 365 days a year. Consumers expect and have come to depend on the real-time availability of financial services, including transaction processing.

14. Op Res refers to the ability of REs to continue providing essential, consumer-facing business services during disruptions. This includes the resilience of business services that rely on outsourcing arrangements. The focus is on consumer-facing services, not on RE's internal services, ensuring no interruption or severe degradation in usability. It is assumed that disruptions will occur through severe but plausible scenarios; there is no probability component since this is not a risk management exercise. For a comprehensive comparison of the Business Continuity Plan versus Op Res, kindly refer to the GN.

15. When disruptions occur in the financial sector, the lack of services can cause significant harm to consumers, extending far beyond mere inconvenience. For consumers, particularly those dependent on real-time financial transactions or critical services like payment processing, any disruption can result in immediate financial losses, the inability to access funds, or missed economic opportunities. The severity of the impact can vary, but in many cases, it can disrupt livelihoods, damage credit ratings, and erode trust in financial institutions.

16. The Op Res lifecycle is composed of the following activities:

a) **Identify important business services** that, if disrupted, could harm consumers or the broader financial sector in Bermuda;

b) **Identify and document** the people, processes, technology, facilities (premises) and information (data), collectively known as 'resources' or 'enablers', that support an RE's important business services **(mapping)**;

c) **Set impact tolerances** for each important business service (i.e., thresholds for maximum tolerable disruption);

d) **Develop internal and external communications plans** for when important business services are disrupted;

e) **Test** the ability to remain within impact tolerances through a range of severe but plausible disruption scenarios, including the development of playbooks;

f) **Conduct remediation** to ensure the RE remains within impact tolerances and **perform lessons learned exercises** to invest in and prioritise activities to increase resilience and respond to disruptions effectively; and

g) **Create** a **self-assessment** document and submit statutory returns that the BMA may require.

17. The following sections outline the requirements for each operational resilience activity.

V. Outsourcing to Third Parties

18. Op Res service delivery is often intrinsically tied to outsourcing. Therefore, operational resilience relies on effective third-party management. This Code establishes requirements for duties, standards, procedures and principles for an RE to adhere to in managing outsourcing arrangements prudently and in alignment with regulatory expectations, mainly:

a) Establishment of standards for the governance and oversight of outsourcing arrangements, including setting clear responsibilities for senior management and the board;

b) Assessing and monitoring of potential risks associated with outsourcing activities, including, among others, operational, reputational, concentration, and compliance risks, as well as sub-contracting/sub-outsourcing/chain outsourcing arrangements of third-party service providers;

c) Ensuring transparency in the relationship between an RE and its third-party service provider(s) and that adequate measures are in place to hold service provider(s) accountable, including for the sub-contracting/sub-outsourcing/chain outsourcing arrangements of the third-party service provider;

d) Ensuring that outsourced services comply with all relevant financial regulations and that the Authority has sufficient access to inspect and supervise an RE's outsourcing arrangements;

e) Safeguarding consumers against the failure of a third-party service provider, as well as ensuring security and privacy of data; and

f) Ensuring that REs have contingency arrangements identified, planned, and, where practicable, in place to enhance operational resilience.

19. For the material outsourcing definition in the GN, an activity shall generally be regarded as a critical activity by an RE if a defect or failure in the provision or performance of that activity would materially impact the RE. For example:

- Business operations, reputation or financial performance
- Ability to manage risk
- Compliance with applicable Bermuda laws
- Clients, policyholders and customers
- Dependent third parties

20. An RE must consider whether outsourcing to another member of the group or related company should be regarded as material.

VI. Board-Level Governance of Op Res and Outsourcing

21. The Board of Directors (board) and senior management team are accountable for Op Res and responsible for the delivery of operational resilience outcomes. This includes initial assessment, vetting, oversight and monitoring of outsourcing arrangements in line with strategic objectives, operational tolerances, risk appetite and regulatory requirements.

22. The board should assume that disruptions will occur and consider this in its statement of risk appetite.

23. The board or delegated responsible party must receive regular updates and clear management information detailing the overall Op Res status, activities underway and their outcomes. The board or delegated responsible party must have adequate knowledge and experience to provide effective oversight and challenge senior management.

24. The board or delegated responsible party must review and approve, at least annually, the list of important business services identified and the impact tolerances that have been set for each.

25. The board or a delegated committee must review Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs), including those associated with outsourcing, along with the results of their regular testing, to ensure they remain appropriate.

26. The board or delegated responsible party is responsible for ensuring that the RE incorporates provisions within its business continuity arrangements to ensure the retention and accessibility of all records essential for sustaining business operations, fulfilling statutory obligations, and providing necessary information requested by the Authority to exercise regulatory powers or carry out supervisory functions.

27. The board or delegated responsible party must review and approve the identified severe but plausible disruption scenarios. This should be undertaken at least annually.

28. The board or delegated responsible party must review and approve a risk management policy for outsourcing at least annually.

29. The board or delegated responsible party must review the operational resilience testing outcomes at least annually and discuss and approve any plans, mitigating measures, or investments required to improve resilience and maintain important business services within tolerance.

30. The board, senior management and the appropriate committees, if applicable, should have timely access to Management Information (MI) or independent reports of sufficient quality and detail to ensure adequate governance, oversight, challenge and informed decision-making.

31. The board or delegated responsible party must approve all material outsourcing arrangements. In addition, the board or a delegated committee must regularly review reports on outsourcing arrangements.

32. The board or delegated responsible party should review and approve, on an annual basis, the self-assessment(s) or statutory return(s) that the RE is required to file with the BMA.

33. The board, senior management, or a delegated responsible party approved by the BMA is responsible for ensuring that the RE notifies the Authority of any significant developments when or before they occur.

VII. Operational Resilience and Outsourcing Management

34. REs must have policies, procedures and controls to implement resilience measures and ensure that essential business services remain within tolerance.

35. REs must have clear roles and responsibilities for implementing and managing operational resilience. REs have the flexibility to use existing oversight and management committees

and structures and extend their scope where possible or establish specific committees and structures for operational resilience as long as they are effective in fulfilling their role.

36. REs must create, maintain and update playbooks for remediating operational outages or service failures as part of Op Res management.

37. Management must draw up a yearly Op Res plan that includes timely service provision, mapping review, testing, mitigation or resilience improvement activities, and annual filing returns.

38. REs must retain meeting minutes, tests, testing outcomes and self-assessments for a minimum of five years from the date of completion and make these documents available to the BMA upon request.

39. Management must also have in place specific outsourcing policies and procedures that include:

a) A risk appetite statement for outsourcing activities and what activities constitute outsourcing at the RE;

b) Criteria for determining what constitutes a material outsourcing at the RE;

c) The evaluation process as to whether and how an activity shall be outsourced;

d) The due diligence to be undertaken in selecting an appropriate service provider;

e) The structure and content of the outsourcing arrangement between the RE and the service provider. Outsourcing relationships must be governed by written agreements that clearly detail all material elements of that arrangement; and

f) The ongoing management and monitoring of outsourcing arrangements post-implementation.

40. While activities can be outsourced, responsibility for those outsourcing activities remains with the board and management. The RE should always seek to ensure that an outsourcing arrangement does not impede the RE's obligations to its customers and regulators.

VIII. Outsourcing Due Diligence, Risk Management and Agreements

41. The board is responsible for reviewing, approving, and overseeing the implementation of a robust risk management process by senior management for evaluating, selecting, and monitoring outsourcing vendors.

42. An RE's board-approved outsourcing policy must contain procedures for the ongoing assessment of service providers' performance, including the day-to-day oversight, changes

to an outsourcing arrangement or service provider (i.e., to its financial position, organisational or ownership structures, sub-outsourcing, or sub-contracting), independent review and audit of compliance with legal and regulatory requirements and policies, and renewal processes.

43. The RE should be able to satisfactorily demonstrate that it has adequate oversight of all its outsourcing arrangements on an ongoing basis. The level of monitoring for each outsourcing activity should be proportionate to the risks the RE faces from pursuing that arrangement.

44. An RE's outsourcing policy must contain a process for sharing risk assessments and reports on all outsourcing arrangements with the board.

45. An RE must establish and maintain policies, procedures, and controls to identify, assess, monitor, and mitigate concentration risk associated with outsourcing arrangements. Concentration risk in outsourcing may arise due to the following:

a) Multiple arrangements with the same or closely affiliated service providers;

b) Reliance on a dominant service provider that is challenging or impossible to replace; or

c) Dependencies wherein unrelated service providers rely on the same subcontractor for service delivery.

46. An RE that is part of a group should also consider the impact of any group-wide aggregate exposures on its management of concentration risk.

47. The RE must undertake a risk evaluation process before entering into an outsourcing agreement. This should include the rationale(s) supporting outsourcing decisions, benefits and how risks arising from the arrangement will be mitigated or managed.

48. Senior management is responsible for ensuring due diligence on potential outsourcing vendors to evaluate their financial stability, operational capabilities, regulatory compliance and track record.

49. The RE and the outsourcing service provider must execute a legally binding written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement.

IX. Identifying Important Business Services

50. A business service is a service that an RE provides to external consumers and delivers a specific outcome. Important business services are those that, if disrupted:

- Can cause unacceptable 'harm' to consumers, depositors or policyholders
- Can cause unacceptable 'harm' to other stakeholders
- Pose a risk to Bermuda's financial stability

51. An RE must identify its important business services.

52. Since the scope of operational resilience is important business services to external consumers, REs must not identify internal services in isolation (e.g., payroll) as an important business service. If internal services are necessary to enable the delivery of important business services, these must be included as processes during the mapping of underlying 'resources' and tested as such. Please refer to the relevant sections 'X. Mapping of Resources' and 'XIII. Testing' within this Code.

53. When in the process of assessing whether business services are important or not, REs must, at a minimum, consider the following factors:

a) Substitutability – i.e., the ability for consumers to obtain the same service or achieve the same outcome through other channels or other REs/service providers;

b) Dependence – e.g., a unique service or consumer base solely dependent on that service. This ties in with substitutability;

c) Time criticality – i.e., the ability for consumers to have the same outcome within comparable time frames;

d) Customer base, both in terms of size and nature, i.e., more susceptible to harm from a disruption (e.g., vulnerable customers);

e) Possible significant disruption to other financial entities, counterparties or critical national infrastructure; and

f) Exit strategies, including resuming the service in-house (insourcing) or transferring to a new service provider.

54. When identifying its important business services, an RE must not identify a collection of services as a single important business service.

55. REs must identify each distinct relevant service separately and ensure due process is followed for each to comply with this Code.

56. The RE's board and senior management should consider whether the number of essential business services identified is commensurate with its size, business nature, customer base and complexity.

57. REs must be able to identify the users of the important business service collectively as a distinct group, not individually. This is necessary to be able to:

a) Clearly articulate the impact of disruption;
b) Establish and test impact tolerance metrics; and
c) Have effective governance from the board and senior management.

58. An RE must review its list of important business services in the following circumstances:

a) If there is a material change to the RE's business or the market in which it operates; and
b) In any event, no later than one year after the previous relevant assessment.

59. REs must also identify important business services that are delivered by a related entity, such as another member of the group, or in conjunction with a related entity or part of the group.

X. Mapping of Resources

60. An RE must identify and document the following 'resources' (enablers) required to deliver each important business service:

a) People;
b) Processes;
c) Technology Systems (IT Systems);
d) Information (Data); and
e) Facilities (Premises).

61. The mapping of services to resources must be documented in sufficient detail to ensure the RE has usable information for subsequent testing, identification and remediation of vulnerabilities, prioritisation, and resilience investment decisions.

62. REs are expected to remain resilient and within impact tolerance, regardless of whether they use third parties.

63. REs must map the resources necessary to deliver important business services, whether provided internally, as part of intra-group arrangements, or externally through third-party service providers.

64. As part of the mapping exercise, REs must identify the intra-group counterparties and third parties providing important business services.

65. REs must have adequate oversight of intra-group and third parties and obtain assurance of service resilience, i.e., the service provider can provide the service both during Business as Usual (BAU) and during a severe but plausible disruption. Oversight must be proportionate to the materiality of the outsourcing.

66. An important business service may be delivered as the outcome of several internal services or activities. Internal services must be mapped as part of the 'process' resource. REs must ensure that internal services are resilient because if they fail, the important business service also fails. In conjunction with the other four types of resources, process resources are tested for resilience. (Please refer to section 'XIII. Testing' within this Code).

67. The mapping exercise must be reviewed by senior management and approved by the board.

68. The mapping exercise must be reviewed on an annual basis or in the event of the following;

a) A material change to the RE's business;
b) New important business services have been identified;
c) Major changes in resources previously mapped;
d) Changes in the impact tolerance thresholds; and
e) Any other change deemed to render the mapping out of date.

XI. Setting Op Res Impact Tolerances

69. Impact tolerance is the maximum level of disruption to an important business service that the RE can tolerate, as measured by length of time, in addition to other metrics. It is assumed that disruption will occur.

70. An RE must set at least one impact tolerance metric for each of its important business services. The minimum mandatory impact tolerance metric is MTPD (Maximum Tolerable Period of Disruption).

71. To assess whether the impact tolerance for an important business service is appropriate, REs must be able to identify the end users (collectively as a group) consuming that service. This ties in with the rationale in the section 'IX. Identifying Important Business Services' within this Code.

72. REs may use other metrics in addition to time, as long as the impact tolerance metrics and their purpose are clearly stated. REs must assess whether other metrics used in conjunction with time would be more appropriate.

73. REs must consider the possibility of several important business services being impacted by disruption simultaneously due to a common cause and a shared underlying resource being affected. While this exercise is not intended to be overly complex, simultaneous disruption should only be considered where it adds value to the RE's operational resilience planning and testing.

74. REs should consider setting different MTPDs for different outcomes. For example, the MTPD impacting a customer may be a certain number of hours, and the MTPD impacting a counterparty may be one day or 24 hours.

75. REs considered systemically important must set an MTPD of when service unavailability poses risks to Bermuda's financial stability.

76. REs must ensure that they can remain within the impact tolerance for each important business service in the event of a severe but plausible disruption scenario.

77. REs must ensure that they do not harm customers in other ways or aggravate the situation (e.g., through contagion risks from a cyber and financial sector perspective, incorrect data or other regulatory breaches) in order to remain within impact tolerance.

78. REs must notify the BMA within 24 hours when they fail to keep important business services within impact tolerance.

79. REs must review their services' impact tolerance when:

a) There is a material change to the important business service;
b) There is a material change to the RE's business; and
c) On an annual basis or not later than one year after the previous assessment.

XII. Communication Plans

80. REs must have a communication strategy to respond to, manage and mitigate disruptions.

81. The communication strategy must include internal and external communication plans for all the severe but plausible scenarios the RE envisages for its important business services.

82. The communication plans must provide clear, timely and relevant information (i.e., cause, extent and impact) to stakeholders. Stakeholders include, but are not limited to, customers, third parties and vendors, intra-group, counterparties, shareholders, regulators, emergency services and the press.

83. REs' communication plans must include:

a) Escalation paths and timeframes/other triggers for escalation; and

b) Decision makers, key individuals, main contacts at suppliers, counterparties, regulators, et al.

84. Where appropriate, external communication must include warnings and/or updates where only indirect communication is possible (e.g., website splash page).

85. Communication plans must be tested as part of scenario testing, and key vendors must be included in the communication plan tests.

XIII. Testing

13.1 Identifying Severe but Plausible Disruption Scenarios

86. REs must identify severe but plausible disruption scenarios that will be used to test the ability to remain within the impact tolerances set (please refer to Section XI. Setting Op Res Impact Tolerances') for the important business services identified. This will help identify areas where further resilience is required. Please refer to the GN on possible disruptive scenarios and other factors to consider.

13.2 Test Plans and Testing

87. REs must develop and document test plans. Test plans must have sufficient details to demonstrate how each important business service will remain within impact tolerance.

88. REs must take account of the following factors when designing test plans:

a) Where possible, testing each underlying resource or related activity that underpins or enables a service;

b) Testing resources in terms of availability and integrity where applicable (e.g., data). Failing the integrity component for a service is considered failing the test;

c) The inclusion and testing of relevant key vendors;

d) The inclusion and testing of relevant communication plans; and

e) The most appropriate way to test each scenario, i.e., desktop walkthrough, simulations, test systems, live systems, etc.

89. Under the requirements of this Code, each scenario should be considered and tested on a stand-alone basis. REs should consider testing the occurrence of multiple disruptive scenarios as simultaneous or concurrent events.

90. Testing plans must be reviewed annually and kept up to date.

91. REs must regularly test their ability to remain within impact tolerances at a minimum by reviewing the following information:

a) When there is a significant change in the RE's business;

b) When there is a significant change in an important business service;

c) When there is a significant change in the underlying resources that underpin an important business service;

d) When new important business services are identified;

e) Following changes and/or improvements made by the RE as a result of previous tests; and

f) On an annual basis.

92. Testing should be repeated under varying levels of disruptive scenarios to go beyond established impact tolerances. Specifically, the RE testing should provide clear indicators of the severity levels at which tests fail, and where impact tolerances are breached.

93. The board, senior management and any appropriate committees must have access to test results and outcomes. This information must be used for, but not limited to:

a) Prioritising the nature and frequency of further tests;

b) Judging whether failing to remain within the impact tolerance in specific scenarios is acceptable and be able to explain the reasoning internally (e.g., Enterprise Risk Management (ERM) and to the BMA;

c) Prioritising any mitigating actions or investment required;

d) Understanding the risks that failed services (and, in turn, the RE) pose to the wider financial sector; and

e) Understanding the risks that failed services pose to customers, including borrowers, depositors and policyholders.

94. Testing must not be conducted in a manner that risks jeopardising live systems and services.

95. REs should have arrangements to test disruptive scenarios in conjunction with their key suppliers. REs should obtain assurance through vendor assessment and management, on the level of service and reliability that key vendors provide. Levels of third-party services should be commensurate and adequate to support the RE's impact tolerance thresholds.

96. REs cannot rely on third-party testing on their behalf if the scenario being tested is disrupted due to a third party's unavailability.

97. Where an RE engages a third party to conduct scenario testing on its behalf, the RE remains responsible for the validity and accuracy of the test, its execution, and the results. The RE,

and not the vendor providing the service nor the third party conducting the testing, is responsible for remaining within impact tolerance.

98. The requirements above pertaining to third parties also apply to intra-group arrangements for the provision of services. REs must assess and manage risk, have adequate oversight of and conduct testing on intra-group arrangements, whether the arrangement is deemed to carry less risk or not.

13.3 Remediation

99. REs should use testing outcomes and other relevant MI in order to improve resilience. REs must take appropriate remedial action to overcome identified limitations and failures which prevent important business services from remaining within impact tolerances.

100. Remediation plans should be implemented and tested within a timeframe that appropriately considers the impact of disruption to the important business service and the nature and extent of improvements required. Remedial actions should not jeopardise the business-as-usual provision of the important business service. REs should share remediation plans, including timeframes, with the BMA as part of the RE's open and proactive engagement with the Authority.

101. Where several important services have failed impact tolerance testing, REs should prioritise remedial actions, taking into account the nature of the service, customer base, logical sequencing (such as interdependencies), and how far out of tolerance the service is considered to be. All other factors being equal, services that are most out of tolerance should be remediated first, i.e., the highest risk factor takes priority.

102. Remediation should extend to the 'resources' that caused tests to fail. This includes individuals fulfilling key roles. REs must ensure they have plans in place (short-term substitutability and long-term succession plans) for key people becoming unavailable.

103. If testing identifies weaknesses and vulnerabilities in the outsourcing arrangements with third parties (including any sub-contracting or sub-outsourcing), the RE must collaborate with the third parties in question to implement mitigating measures and ensure the important business service stays within tolerance during severe disruption.

XIV. Lessons Learned

104. REs must put in place activities and processes in order to incorporate into the REs' operations all lessons learnt to improve resilience.

105. The lessons learned or continuous improvement processes are the last step in the cycle and should cover the following components:

a) Governance;
b) Identifying important business services;
c) Mapping of resources;
d) Setting impact tolerances;
e) Communication plans; and
f) Testing.

Therefore, REs must endeavour to keep improving all aspects of Op Res.

106. Testing outcomes and remediation constitute a prominent aspect of lessons learned. Please refer to 'Testing' (Section XIII) item 13.3 Remediation. In addition, REs should conduct a lesson- learned exercise in the aftermath of a real-world disruptive event on an important business service to evaluate that the service remained within tolerance as expected. If not, the RE should identify and measure the variance between real-world events and simulation/testing.

107. The variance from testing should demonstrate whether the testing was realistic in scope, resources and assumptions made and whether test execution was accurate.

108. REs should review and improve test plans if a real-world disruption invalidates a previous 'within tolerance' test result. Revised test plans must be re-run and validated.

XV. Self-Assessment and Returns

109. REs are required to make their annual self-assessment available to the BMA to demonstrate adherence to this Operational Resilience Code.

110. The self-assessment should contain:

a) A brief description of the methodology used to undertake Op Res activities;
b) The list of important business services identified and impact tolerance metrics;
c) The rationale for how impact tolerance and other metrics were set;
d) The list of severe but plausible disruptive scenarios that were considered;
e) The testing carried out and testing outcomes; and
f) Resilience improvement measures put in place following testing.

111. For systemically important Op Res, the self-assessment should also contain information on the mapping of resources and services.

112. For important business services that are outside impact tolerance thresholds, the self-assessment must describe the actions the RE is planning or undertaking to bring the services within impact tolerance and provide timelines for completion.

113. For entities forming part of a Group, the self-assessment must include intra-group services, i.e., services obtained from other entities within the Group or services rendered to the Group.

114. The board is responsible for reviewing and approving the self-assessment prior to submission.

115. The BMA may require REs to demonstrate the resilience of specific important business services for specific severe but plausible disruption scenarios. In this case, the BMA will:

a) Select and communicate the details of the disruptive scenario to the REs;
b) Set out the resilience testing expected and other documentation artefacts; and
c) Set out timelines for submission filing.

116. REs submitting a filing return on a BMA-specific scenario are not required to submit the self-assessment for that reporting year.

117. REs should retain the self-assessment and other filing return documentation for a minimum of five years from the date of completion and make it available to the BMA upon request.

XVI. Implementation

118. REs are required to adhere to the requirements set out in this Code by 31 March 2028, except for REs licensed under the BDCA, which are required to adhere to the requirements by 31 March 2026.

XVII. Appendix A - Glossary of Terms

BAU – Business As Usual
BCP – Business Continuity Planning
CNI – Critical National Infrastructure
DRP – Disaster Recovery Planning
MI – Management Information
MTPD – Maximum Tolerable Period of Disruption
Op Res – Operational Resilience
RE – Relevant Entity
RPO – Recovery Point Objective
RTO – Recovery Time Objective

BERMUDA MONETARY AUTHORITY

OPERATIONAL RESILIENCE AND OUTSOURCING GUIDANCE NOTES

CORPORATE SERVICE PROVIDERS, TRUST BUSINESSES, MONEY SERVICE BUSINESSES, INVESTMENT BUSINESSES, FUND ADMINISTRATION PROVIDER BUSINESSES, BANKS AND DEPOSIT COMPANIES, DIGITAL ASSET BUSINESSES, COMMERCIAL INSURERS, IIGB AND IILT INSURERS, INSURANCE MANAGERS, INSURANCE BROKERS, INSURANCE MARKETPLACE PROVIDERS AND AGENTS

January 2025

Table of Contents

Operational Resilience and Outsourcing Guidance

This Guidance Notes (GN) document should be read in conjunction with the Bermuda Monetary Authority (Authority or BMA) Operational Resilience and Outsourcing Code (Code).

1. Introduction

Relevant Entities (REs) are increasingly globally interconnected when providing financial services to customers. In addition, the delivery of financial services is 'always on' 24 hours a day, 365 days a year. Customers expect, and have come to depend upon, real-time availability of financial services and transaction processing.

As a result, when disruptions occur, they can quickly result in harm to customers, well beyond causing temporary inconvenience. Potential harms not only include negative financial and mental health impacts on individual customers. They also include risks related to contagion to the wider financial sector and the speed at which it may occur.

The Authority has made progress towards mitigating this through the introduction of Codes of Conduct for Cyber Risk Management and through the introduction of Outsourcing Guidance. However, these are only elements of operational resilience (Op Res) and do not consider the wider implications (i.e. a lack thereof) for Op Res of relevant entities.

REs are already expected to have Business Continuity Plans (BCP) in place and to test these plans regularly. These plans are often 'firm centric', with the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) set to suit the RE's risk appetite rather than tailored to customers' expectations and/or needs.

A conventional BCP often has gaps in service while recovery is underway, influenced by the RTOs and RPOs that have been set. In addition, underpinning BCP activities is a risk management exercise assessing the probability of disruptions occurring. Operational Resilience, however, is different, in that it is more holistic and customer centric.

Although the development of Op Res was driven by historical technology and cyber incidents, it is not limited in scope by either of these events. Additional events included contending with and overcoming supply chain interruptions and third-party failures, geo-political uncertainty brought on by wars and terrorist attacks, and the global COVID-19 pandemic, including shut-downs.

Op Res is the capability of organisations to keep delivering business services that are important to their customers throughout a disruption. Its emphasis is on customer- facing services rather than the interruption, or serious degradation, of an organisation's internal services. Op Res also assumes that severe but plausible scenarios that cause disruption will occur; there is no probability component as this is not a risk management exercise.

Op Res is frequently confused with Operational Risk. Organisations, including regulated entities, can capitalise against operational risks, but they cannot effectively capitalise against the lack of operational resilience. Operational risk focus is on identifying potential errors or failures in an organisation's operational processes and has a regulatory focus on compliance and internal controls.

Op Res is about maintaining the delivery of key services through adversity and disruptions. It also encourages organisations to have a 'resilience by design' mindset, where resilience becomes ingrained throughout all levels of operations rather than an afterthought. The focus of the Code is on testing and improving Op Res to cope with severe but plausible disruption scenarios. This focus

allows the Authority to assess, in a repeatable, consistent manner, whether REs are sufficiently resilient.

Scope	
Operational Resilience	**BCP and IT Disaster Recovery (IT DR)**
Op Res and Outsourcing Code	Cyber Codes of Conduct
• Op Res considered an additional area that requires oversight within existing structures and/or new roles and structures, as long as governance is effective	• Governance and Enterprise-wide Risk Management (ERM) required for BCP, IT DR and outsourcing. This is also present as a requirement in other Prudential Codes
Op Res • Focus is resilience only, i.e., continuing to provide an acceptable level of service without interruption and without services being degraded to a point where they can be considered unfit, despite suffering a severe but plausible disruptive event • Goes beyond IT systems/data and requires mapping the underlying People, Processes, and Facilities that underpin the delivery of the service. These five elements are collectively known as 'resources' or 'enablers'	**IT DR** • May mean there is an event that causes an interruption which in turn requires recovery • Business continuity may be both through resilience and recovery • IT DR focus is the recovery of IT systems/data (as the acronym implies)
Important Customer Facing Services • Focuses on important customer facing services that can cause 'harm' if unavailable for extended periods of time • Customer centric • 'Harm' is different than an inconvenience or disruption that is rectifiable in the short or medium term • The main, mandatory metric is time, which is expressed as Maximum Tolerable Period of Disruption (MTPD). REs are free to use additional metrics	**Business Processes** • BCP focus is the continuity of business processes where processes can be internal or external • Must cater to various magnitudes and severities of disruptions • Focus is on business priorities with business-appropriate metrics in terms of RTO, RPO, etc. • Business-centric priorities can be both internal and external facing, e.g., payroll
Resilience • The core premise is that disruptive events WILL happen to important services and therefore the RE needs to plan to be resilient accordingly. Does not require taking probability and frequency into account	**Risk Management** • Comprises Operational Risk Management elements with impact, probability and frequency

Extended Vendor Management • Mapping/understanding the five resources underpinning an outsourced Important Customer Facing Service • Better understanding of sub-outsourcing to fourth/fifth parties if necessary	**Vendor Management** • Vendor management/outsourcing/third party oversight
Communication Plans • Explicitly introduces the requirement for internal and external Communication Plans	**Communication Plans** • Communication may be part of playbooks but are not always considered
Testing • Applies to important services • Includes the underpinning resources • Explicitly involves the vendors and vendors' resources • Applies to severe but plausible scenarios • Testing beyond (i.e., finding the limit where the RE cannot remain within MTPD) • Includes the Communication Plan	**IT DR / BCP Testing** • Tests IT systems/data and business priorities • May include some elements of underpinning resources • Vendor not always involved/considered • Scenarios vary in magnitude • Aims to recover and stay within business specified metrics (which may or may not include time)
Lessons Learned • Wider organisational/customer facing lessons learned	**Lessons Learned** • IT and possibly business centric lessons learned

The Op Res lifecycle is composed of the following domains or activities:

a) **Identify important business services** that, if disrupted, could cause harm to consumers or wider financial sector in Bermuda;

b) **Identify and document** the people, processes, technology, facilities (premises) and information (data), collectively known as ‘resources’ or ‘enablers’, that support an RE’s important business services (i.e., mapping);

c) **Set impact tolerances** for each important business service (i.e., thresholds for maximum tolerable disruption);

d) **Develop internal and external communications plans** for when important business services are disrupted;

e) **Test** the ability to remain within impact tolerances through a range of severe but plausible disruption scenarios;

f) **Remediate** to ensure the RE remains within impact tolerances and **conduct lessons learned exercises** to invest in and prioritise activities that increase resilience and respond to disruptions effectively; and

g) **Create a self-assessment** document and/or submit any statutory returns that the BMA requires.

For each domain, detailed guidance on the regulatory requirements, approach, expected outcomes and factors to consider, is described in the sections below.

2. Board Level Governance of Op Res and Outsourcing

The board is responsible and accountable for the operational resilience of the RE. The board's role in operational resilience is in line with the overall board's function, i.e., to set risk appetite and to provide oversight and adequate challenge. The board, though not experts, should collectively have adequate knowledge of operational resilience and have access on a regular basis to the latest Management information (MI) on Op Res. The board will need to decide on and prioritise resilience initiatives, which require timely, high-quality, relevant MI.

A detailed list of what the Authority requires from the board is in the Code. The board must review and approve, on an annual basis, the documentation generated through the main elements of the operational resilience lifecycle, i.e.:

- Identify important business services
- Map resources
- Set impact tolerances
- Test (including testing the communication plans)

All elements of the Op Res lifecycle are covered in detail, in subsequent sections of this GN. Specifically, the board should review and approve the self-assessment and any statutory return required by the BMA, prior to submission.

The board may appoint specific senior management roles, oversight committees and other roles as necessary to manage Op Res and may execute initiatives and activities aimed at increasing operational resilience. It is at the discretion of the board and senior management whether new senior roles and oversight committees are required or whether operational resilience is included within the scope of existing roles and oversight structures. The overriding factor is to ensure the oversight and management of Op Res is effective. It is the BMA's expectation that the oversight, management, processes and procedures for Op Res are sufficiently detailed, adequate and proportionate to the nature of the firm's business, nature, size and complexity.

Note: The Operational Resilience and Outsourcing Code covers a wide variety of entities in terms of size, nature of business, and services offered. Regulatory requirements that apply to larger entities that provide a time/dependency-critical, customer-facing service may not apply to smaller entities. Entities should ask themselves the following questions:

- Is a sizeable customer base being served?

- Are the services provided time critical (i.e., would an interruption in minutes or hours causes unacceptable 'harm' to consumers?)

- Does a customer-facing service, if disrupted, pose a contagion risk to Bermuda's financial stability?

If the answers to the questions above are 'No', then the entity has no service that falls under the definition of an important business service that must be operationally resilient. In these cases, unless the nature of the business changes over time, annual reviews of services, disruption scenarios, and self-assessment would be nil. For further details, please refer to:

- Section '9. Identifying Operational Resilience Important Business Services' within the Code

- Section '6. Identifying Operational Resilience Important Business Services', bullets (a) to (f) with this GN

Notwithstanding the Op Res note above, entities are still obliged to comply with the clauses related to outsourcing and third-party oversight.

3. Outsourcing Materiality, Due Diligence and Risk Management

Defining what constitutes outsourcing and, consequently, material outsourcing by management in each RE will be essential for developing a credible risk-based approach to managing outsourcing risk. Not all activities outsourced will be critical activities; therefore, management will need to determine the factors that should be used to assess which activities are critical. For example, if the delivery of an activity that has been outsourced is considered 'time critical', then criticality could be defined based on the length of time a service is not available before it damages the business's reputation, impedes the delivery of important business services, or causes a regulatory breach or material financial loss. These could be appropriate metrics for determining the criticality in this case. Whatever metrics are used to determine materiality, they will need to be formalised and clearly articulated in the RE's policy and procedures, with senior management able to explain the rationale for choosing them.

Where the activity being outsourced is deemed by the RE's management not to be a critical activity, the implementation of the Code provisions can be applied proportionally to the risk that a failure in the delivery of that outsourced service would pose to the RE from a financial, regulatory, and reputational perspective. The RE will need to satisfactorily explain why it is appropriate and proportionate not to fully apply those provisions.

The BMA expects the RE to undertake a risk evaluation process prior to entering an outsourcing arrangement. As part of this process, the Authority expects the RE to clearly articulate the rationale(s) for the outsourcing decisions. As such, this evaluation must set out the benefits of outsourcing and how any risks arising from the arrangement are to be mitigated/managed. There will be a specific focus on this risk evaluation by the Authority in cases where:

a) A material outsourcing is being contemplated or re-negotiated; or

b) Multiple activities are to be or have been outsourced to a single service provider, given the heightened concentration risk to which the RE would be exposed.

Subject to the Code and its related Guidance, 'purchased services' are services that are deemed not to be outsourced and are mainly services that other companies provide to the RE and are not part of the services and activities provided by the RE itself. Examples of purchased services include:

- The supply of external advisory services to the RE that do not form part of the services and activities of the RE

- Provision of external legal advice to the RE

- The provision of external training for staff

- The external security, management and maintenance of an RE's premises and personnel

With regard to the purchased services definition above, if a trust company that is acting as trustee arranges the supply of investment management services to a trust, this could fall within the above definition, depending on individual circumstances. This activity would generally not be deemed to be outsourcing by a trust company acting as an individual trustee, except in cases where the trust company held itself out as providing investment management services as part of its individual trustee service. However, if the ongoing monitoring of the performance of the investment management company that is providing these services to the trust is outsourced by the trust company and acts as a trustee for another third-party provider, this would constitute outsourcing.

The BMA acknowledges that in certain instances, transferring an outsourced function back to the RE's direct remit may not be commercially or operationally feasible, and may even increase operational risk. When such circumstances arise, the RE faces significant additional risk by relying entirely on the service provider for the provision of these activities. Therefore, the Authority mandates the RE to exercise greater oversight of these arrangements in such cases and to implement appropriate contingency plans for the provision of these services by alternative providers and/or reintegrate the services back into the RE's operations as part of its contingency planning.

Once the risk evaluation process has determined that outsourcing is the preferred option for an activity, the next stage is to conduct appropriate due diligence on the service provider.

This due diligence should include, but not be limited to, evaluating whether the service provider has the following in place:

- The quantity and quality of staff with the requisite skills and experience to effectively deliver the outsourced activities, as well as the requisite legal and other authorisation(s) to perform the outsourced activity reliably and professionally throughout the life of the outsourcing

- The relevant technology, cyber security arrangements, operational infrastructure and financial capacity to undertake the outsourcing arrangement effectively and efficiently

- Appropriate information and data security to protect any and all confidential information relating to the RE and its clients

- An appropriate risk management framework and controls to ensure that the carrying out of the outsourced activity is properly supervised and any risks associated with the outsourcing are effectively managed

- The ability to maintain appropriate internal controls and meet regulatory requirements

- An appropriate BCP and DRP and can demonstrate a successful track record of BCP and Disaster Recovery testing

- The ability to provide access to all documents and data relating to the outsourced activity, its auditors and its competent authority

Additionally, the RE should consider the following:

- The impact of the outsourcing arrangement on its finances, reputation and operations, or a significant business line

- The risk of potential loss, temporarily or permanently, of access to important data

- The degree of difficulty and time required to find an alternative service provider or bring the business activity fully 'in-house'

In cases where the outsourcing is considered material, the Authority will require the following:

- The RE's risk evaluation assessment needs to clearly articulate the benefits and the risks of pursuing this outsourcing option

- Due diligence undertaken by the RE as to the robustness and resilience of the service provider's BCP and Disaster Recovery (DR) plans

- Require more regular testing of these contingency plans at the service provider than for outsourcing where the service can be easily replaced or transferred back to the RE. This increased frequency of testing is to be explicitly included in the written agreement

- More intense monitoring of the performance of the service provider by the RE than for outsourcing, where the service can be easily transferred back to the RE. This increased monitoring is to be explicitly included in the written agreement

- Immediate disclosure, as part of the written agreement, to the RE by the service provider at the point when it first becomes aware of any legal, operational, technological, financial, resource or regulatory adverse development that may affect the service provider's ability to provide the outsourced activity

- Require the development by the RE of more detailed contingency plans that could be utilised if the service provider is unable to provide the outsourced activity. In this case, the contingency plan would relate to the ability to transfer the activity to other service providers in the same jurisdiction in a timely manner

At a minimum, the policies and procedures should include the following:

- An effective method for identifying and quantifying concentration risk exposures related to outsourcing activities, including dependencies on specific outsourcing service providers, geographic locations and critical activities

- Regular risk assessments evaluating the impact of concentration risk on the RE's operations, financial condition and operational resilience

- Robust and enhanced monitoring frameworks for identified outsourcing concentration risks

4. Outsourcing Agreements

Depending on the activity being outsourced, the Authority expects the written agreement to specify the following:

- The activities to be outsourced and laws/regulations applicable to the agreement

- The responsibilities of the RE and service provider in the agreement
- Relevant policies, procedures and controls to ensure the ongoing security and confidentiality of information provided by the RE to the service provider
- An obligation imposed on the service provider to comply with all relevant data protection, and data privacy rules and regulations
- An obligation imposed on the service provider to maintain appropriate risk management standards and internal controls through the life of the outsourcing
- An obligation imposed on the service provider to provide regular updates on its financial soundness, and confirmation that it retains the human expertise, and technological and operational capacity to provide the contracted activities through the life of the outsourcing
- An obligation to impose a material adverse change disclosure on the service provider to immediately disclose to the RE any legal, operational, technological, financial, resource or regulatory adverse development that may affect the service provider's ability to provide the outsourced activity on an ongoing basis
- The agreed upon quantitative and qualitative service level standards and performance targets to be met by the service provider in performing the activities, together with the method and frequency by which these quality standards and performance metrics will be monitored by the RE through the life of the outsourcing
- Specify the reporting and escalation process where performance standards are not met, and the dispute escalation and resolution process agreed upon by both parties
- An obligation on the service provider to provide the RE regular updates on the following:

    a) The adequacy of its BCP and DRP;

    b) Any material changes in its BCP or DRP that would affect the provision of the RE's activity; and

    c) The results of the regular testing of its BCP and DRP (in conjunction with the RE, if requested)

- Whether or not sub-contracting is allowed in the agreement, and the conditions and liabilities imposed on the service provider and the sub-contractor where this is allowed
- The conditions, triggers or thresholds that would allow either party to terminate or exit early from the agreement
- An obligation imposed on the service provider to provide access to all documents and data relating to the outsourced activity to the RE, its auditors and its competent authority, as well as providing access to the business premises of the outsourcing service provider for these parties if required

In the case of both intra-group material and non-material outsourcing, any written outsourcing agreement between the RE and the group service provider may be supplemented with other group

documents (including but not limited to group policy and procedure documents, Performance Level Agreements (PLA) and/or Service Level Agreements (SLA). This is provided the RE can demonstrate to the Authority, if requested to do so, that the provisions contained in the supplemental group documents are sufficiently robust and can be relied on by the RE to deliver the relevant protection/action, as needed.

5. Outsourcing Management Information

Management information should, at a minimum, contain the following:

- A summary of all outsourcing arrangements, detailing the scope, nature and criticality of outsourced activities
- An evaluation of the risks associated with each material outsourcing arrangement, including legal, compliance, reputational, operational and resilience risks
- An overview of the risk mitigation strategies implemented for each material outsourcing arrangement
- An update on the material outsourcing arrangements that are aligned with a board-approved outsourcing risk appetite
- Notification of any material changes to the contractual agreements between the RE and outsourcing service provider for material outsourcing arrangements
- Review of BCPs and DRPs for material outsourcing arrangements
- A summary of the results of the most recent BCP and/or DRP testing, including an overview of remediation efforts in response to any deficiencies identified during the testing
- An analysis of the service level performance metrics as agreed between the RE and outsourcing service provider
- Reporting on any incidents, breaches or disruptions of the material outsourcing arrangements, including any related operational losses and actions to be taken to resolve and prevent future incidents
- An assessment of compliance with regulatory requirements and the reporting of any breaches of these requirements
- Identification of emerging risks and trends in relation to outsourcing, including technological advances, regulatory changes and market developments

6. Identifying Important Business Services

Business services deliver a specific outcome or service to an identifiable user external to the firm and should be distinguished from business lines, which are a collection of services and activities (e.g., a specific product offering).

Banks must identify important business services that may pose a risk to account holders. Insurance companies must also identify important business services that may pose a risk to policyholder protection.

Additional factors not listed in the Code that the RE should consider when identifying its important business services may include:

a) The sensitivity level of the data held;

b) The potential impact on the RE's financial viability if any disruptions to customers occurs;

c) The potential impact of reputational damage to the RE and reputational damage that extends to customers or, in the case of insurance, policyholders;

d) The potential impact on the orderly operation of the wider financial sector;

e) Whether or not disruption to the services could amount to a breach of a legal or regulatory obligation; and

f) Clients that are important to the financial stability of Bermuda.

An RE's important business services will be a relatively short list of external-facing services for which the firm has chosen to build high levels of operational resilience in anticipation of operational disruption.

An RE should not identify a collection of services as a single important business service when identifying its important business services. For example, 'self-service banking' comprises telephone banking, internet banking, mobile apps, and ATMs.

REs should identify each distinct relevant service separately and ensure due process is followed for Code compliance. Continuing with the 'self-service' example above, four distinct services are identified. These may share or have in common underlying 'resources' in terms of people, processes, technology systems (IT systems), facilities (premises), and information (data).

In the case of insurance services, the insurance company should consider providing an appropriate degree of policyholder protection. This protection should mainly concern the impact that a disruption in service may have on policyholders, which in turn depends on the type of product, type of policyholder, and the nature of any adverse effects on the policyholder and the wider market if policies are not honoured.

7. Mapping of Resources

REs are required to identify and document the necessary people, processes, technology systems (IT systems), facilities (premises), and information (data), collectively known and referred to as the 'resources' (enablers) required to deliver each of their important business services. The terms in brackets are used interchangeably with their counterparts within the Code and this GN.

Below is a broader but not definitive description of the resources. However, REs are encouraged to include in their mapping any wider definition of the resources if it better serves the mapping exercise and the quality of the information as the outcome.

- **People** – Under this category, people within the organisation and its vendors support and enable the provision of important business services. These may include key staff and contractors with specific technical skills/knowledge/experience, decision makers and approvers, overall senior management accountable for oversight, and staff responsible for implementing and monitoring controls. Substitutability, knowledge sharing and transfer, teams operating in silos, teams'

strength and size, staff churn, attrition and hiring lead times, skills scarcity and competitor demand for similar skills in the market. Niches, specialised skills and roles that come into play during an incident (e.g., cyber forensic analysis) also should be considered. Please refer to the 'Testing' section and succession planning within this GN.

- **Processes** – A process is a structured set of activities designed to produce a specific output. Organisations should have end-to-end visibility of the chain of processes and activities leading up to and enabling the delivery of important business services. Internal and external processes, as well as internal and external inputs and outputs, should be clearly defined and understood. Processes may be technology-driven or otherwise.

- **Technology Systems** – Information Technology (IT) systems and the underlying architecture that supports the provision of the service. Similar to the processes above, several IT systems may be involved that are interconnected by the flow of data and enabled by the underlying architecture of networks, servers and so forth. Due consideration should be given to the added complexity when IT systems and underlying architecture are provisioned wholly or in part by third parties.

- **Facilities** – Office locations, data centres, printing and mailing centres, credit card production/statements, client communications/helpdesk, Network Operations Centre (NOC), Cash Depot/Vaults.

- **Information** – Any data, feeds or material that is required by an organisation to deliver a service. These may include stock exchange, foreign exchange and other market information feeds. Consideration should be given to whether or not the information is stored in different formats or undergoes several iterations of data manipulation and/or aggregation prior to its use for delivering a service. Refer to '**Processes'** above and related activities.

The level of detail required in the documentation should be proportionate to the size, scale, and nature of the business services offered by the RE. The BMA will not prescribe a rigid approach or methodology. The RE must ensure that the mapping exercise is usable and beneficial to itself.

Intra-group arrangements and third parties increase the complexity of the mapping exercise. These need to be assessed and mapped accordingly. The Code itself provides an extensive explanation of how the firm must comply with regulations irrespective of outsourcing arrangements. The BMA published Outsourcing Guidance and Cyber Codes outlining regulations in this domain.

Intra-group arrangements, sharing group resources and provision by third parties provide benefits to REs, i.e., efficiency, cost savings, expertise, etc. The mapping complexity arises if there is less visibility of how the service provider operates internally, its resources and its own resilience. For intra-group arrangements there may be more visibility in this regard. However, both intra-group and third parties may have conflicting and competing priorities during a disruptive incident when compared to BAU. If a service provider is providing a service to several firms and that service is severely limited during a crisis, particular firms may suffer as a result.

To add a further layer of complexity, third parties may outsource to fourth parties. Though not mandated in the Code, REs should have a clear understanding of how fourth/fifth parties' capabilities may affect the third party's ability to provide an important business service.

An RE is still responsible for ensuring it remains within impact tolerance if a third-party provider fails or causes the firm to be outside of the impact tolerance. However, it is recognised that Bermuda has specific infrastructure limitations, e.g., having one power station and other Critical National Infrastructure (CNI) restrictions. It is acknowledged that there will be instances where firms will be

out of tolerance despite all the resilience put in place, due to circumstances and resources beyond their control.

The internal services that support an important external business service are to be considered and mapped under the 'Process' resource. The chain of internal services performed must be resilient; otherwise, an internal service failure would break the chain and put the important business service out of the tolerance threshold. Testing and improving resilience measures will be required for any resources that put the important business service at risk.

The mapping should be reviewed on an annual basis or when there is a material change. Due to the varying size, nature and complexity of the REs, the BMA intentionally does not prescribe what qualifies as a 'material change'. REs are expected to have their own definition of a 'material change'. In principle, mergers and acquisitions, new business lines, changes in key personnel, changes in key vendors or intra-group arrangements, tighter SLAs by counterparties, and notable premises or facilities changes (e.g., migrating a data centre) should be considered by firms as triggers for a mapping exercise. The exercise should not be done from scratch, but instead factor in recent material changes that have been evaluated.

The expected outcome of the mapping exercise is for the RE to have a clear understanding of all the resources required for each important business service in order to:

a) Conduct testing (i.e., identify and remedy vulnerabilities and shortcomings); and

b) Identify key personnel and develop short-term and long-term plans (i.e. succession planning) should those key personnel be unavailable.

Mapping exercises are expected to be developed and refined after each iteration.

8. Setting Impact Tolerances

Impact tolerance is the maximum level of disruption to an important business service as measured by length of time, in addition to other metrics. Since the main metric is time, MTPD is used to measure this.

As per previous sections of this GN, Op Res is not a risk management exercise. Therefore, neither the cause nor the probability of a disruptive event needs to be defined; instead, it is assumed that the disruptive event will occur.

It is not mandatory to consider the frequency at which disruptive events are likely to occur. Impact tolerance is set for a single disruption. REs may, at their discretion, consider multiple disruptions or frequent disruption scenarios if they help inform the impact tolerance setting exercise. However, it is not the aim of Op Res regulations to introduce unwarranted complexity.

REs must set an impact tolerance for each of their important business services. Again, time should be used as the main and mandatory metric. Additional metrics should be considered for inclusion. Examples include transaction volume, total transaction value, settlement deadlines, and legal and/or regulatory obligations.

Additional factors not listed in the Code that an RE should consider when setting impact tolerances may include the following:

a) The sensitivity of data held and any potential loss of confidentiality, integrity or availability of data;

b) Customers' resulting financial losses;

c) The RE's financial loss and the potential impact on its financial viability in the event of further disruptions to customers;

d) The potential to cause reputational damage to the RE in terms of that reputational damage extending to customers, including in the case of insurance policyholders;

e) The potential impact on the orderly operation of financial markets, including contagion risk;

f) Customer confidence and wider market confidence; and

g) Whether or not the disruption to the services could amount to a breach of legal or regulatory obligations

As the impacts of a disruption should be clear, the customers (users) of the service should be identifiable, e.g. retail customers, market counterparties, business customers, etc. There should be clear demographics or characteristics to identify affected customer groups.

Due consideration must be given to the possibility of a common shared resource (e.g., data centre) being disrupted, which, in turn, causes several important business services to become out of tolerance. This may be particularly relevant where services are shared across organisations that are part of the same group of companies. This is another reason why the mapping of resources must be comprehensive and have an adequate level of detail in order to provide the RE's management with the information they need to take Op Res steps.

REs should also examine the complexity of the services they provide and factor in other variables, such as peak times or peak periods (e.g., Christmas holidays), any periods of time when the firm's existence and viability are most in jeopardy and the period of time when service unavailability poses contagion risks that may impact Bermuda's financial stability.

For insurers, policyholder protection and any adverse effects on the policyholder and the wider market if policies are not honoured should be considered.

The Code states that REs must ensure that staying within chosen impact tolerance during disruption, does not cause harm in other ways. This clause considers the repercussions and unintended consequences that may happen when the primary aim is to remain within impact tolerance per se, rather than focusing on avoiding harm to customers. In certain situations, such as corrupt or incorrect data, cyber-attacks and other scenarios, the risks of keeping a service running are higher than suspending/shutting down the service, which can result in breaching the impact tolerance threshold. A sensible approach must be considered and, when in doubt, discussed with the BMA.

9. Communication Plans

Communication plans have always been an essential component of BCP and IT DR. They are even more crucial for Op Res as its scope is more extensive in terms of planning, scenarios and the number of stakeholders involved. Timely and effective communication during a disruption or crisis is essential for:

a) Co-ordinating internal resilience efforts, including escalation paths and briefing senior management;

b) Co-ordinating with vendors, suppliers, utility providers and emergency services;

c) Keeping the customers/end users up to date with the status and progress of the disruption;

d) Directing customers to alternative services and channels where substitutability is an option;

e) Briefing and co-ordinating with the regulator;

f) Co-ordinating internally to ensure the RE's staff are not independently issuing public-facing statements or updates unless vetted and approved as part of the planned communication channels; and

g) Managing the media, which may include:

   - Issuing press releases and/or conducting interviews through various media channels, as appropriate;
   - Monitoring the media's narrative in the reporting on the disruption;
   - Monitoring social media and providing responses, as appropriate.

An RE must have a communication strategy in place to respond to, manage and mitigate disruptions. The communication strategy must include internal and external communication plans for all the severe but plausible scenarios that the firm envisages for its important business services. These may include pre-planned statements, also known as 'canned responses' tailored for various delivery channels such as tweets, web splash pages, etc.

The communication plans must provide clear, timely and relevant information (cause, extent, impact) to stakeholders. Stakeholders include but are not limited to consumers, third parties and vendors, intra-group, counterparties, shareholders, regulators and emergency services.

REs' communication plans must include:

a) Escalation paths and timeframes/other triggers for escalation; and

b) Decision makers, key individuals and main contacts at suppliers, counterparties, regulators, et al.

Communication is more effective when it includes the time or time interval between updates (e.g., every two hours on the hour). The communication update schedule should be strictly adhered to. Even when there are no changes to report, the updates should be released stating this. Regular and clear updates engender trust amongst stakeholders and provide the narrative from the RE's perspective.

Where appropriate, external communication must include warnings and/or updates if only indirect communication is possible (e.g., website splash page).

Communication plans must be tested as part of scenario testing. Key vendors must be included in the communication plan tests.

10. Testing

10.1 Identifying severe but plausible disruption scenarios

As described in the Code, the next stage after setting impact tolerances for the important business services, is to test the ability to remain within tolerance when severe but plausible disruption scenarios occur.

It is assumed that disruptions will occur. Consequently, as previously discussed, Op Res is not a risk management exercise in assessing probability. Therefore, the focus of testing should not be incident prevention but resilience. REs need to focus on how they will continue to provide important business services at an acceptable level (i.e., with services not degraded to an extent to be considered unusable or interrupted) despite suffering a severe but plausible disruption scenario.

Identifying the scenarios to be considered for testing is an important exercise in and of itself. REs should consider the following:

a) The nature of the business;

b) The local environment they operate in, in terms of vendors (limitation of), counterparties, natural phenomena such as hurricanes, telecoms and utilities such as electricity;

c) Any previous incidents within the RE, the wider group if applicable, the financial sector within its home jurisdiction, and other jurisdictions where it operates;

d) Group considerations, if applicable, such as shared infrastructure and other dependencies, group incident support, SLA agreements and group priorities;

e) Upstream and downstream obligations (e.g., settlement, policy handling for insurers);

f) Regulatory and legal requirements and compliance;

g) Reputational risk.

Possible disruptive scenarios that REs should consider among others, are:

a) Corruption, deletion or manipulation of data critical to the delivery of its important business services (also refer to the Cyber Code of Conduct);

b) Unavailability of facilities, premises or key people;

c) Unavailability of third-party services or vendors, which are critical to the delivery of its important business services;

d) Disruption to, or by, other market participants or market contagion;

e) Loss or reduced provision of technology or the IT services that underpin the delivery of important business services;

f) Unique points of failure (e.g., utility supplies, Critical National Infrastructure);

g) Dependency on Group and vice-versa, as applicable;

h) Catastrophic natural events such as hurricanes, earthquakes and pandemics; and

i) Political disruption such as civil unrest, riots and war.

10.2 Test plans and testing

Test plans provide a documented, repeatable way of gaining reassurance on the level of resilience for important business services. Initial tests are used to establish a baseline. It is expected that tests will evolve in detail, complexity and realism after each iteration, as lessons learned are fed back into the test design. Any test assumptions should be realistic and not a shortcut to test success, i.e., to stay within impact tolerance as the scope of operational resilience is severe but plausible scenarios.

In addition to the test plan design considerations listed in the Code REs should also consider:

a) The size and complexity of the RE itself and the wider group, if applicable. A proportional approach is expected. Some REs will identify more services and more disruptive scenarios than others., which would result in undertaking considerably more tests;

b) Substitutability of services and resources is a requirement in the Code itself. This should be noted by REs subject to the Code;

c) The frequency with which changes are made to operations or particular services and associated underlying resources. These changes should drive the frequency of testing; and

d) How often the operating environment changes in terms of the financial landscape, vendors, utilities and the natural environment. Environmental changes, in turn, could also give rise to different threats or disruptive scenarios and, therefore, should also be considered.

Adequate oversight of third parties and the involvement of third parties in testing is key. The Code outlines People, Processes, Technology Systems (IT Systems), Information (Data) and Facilities (Premises) as the five resources (or enablers) underpinning an important business service. Any of these resources may be outsourced by an RE to third parties, including other members of a group of companies. The *Cyber Code of Conduct* and *Outsourcing Guidance* mainly set out Technology Systems and Data outsourcing regulations. The *Operational Resilience and Outsourcing Code* extends and sets out vendor oversight expectations for People, Processes, and Facilities.

REs should also consider vendors' own impact tolerances, as well as fourth and fifth-line vendors (i.e., the vendor's vendors and the vendor to the vendor's vendor), especially in cases of commonality where contagion is possible (e.g., vendors within the same building/premises, vendors using the same products or hosted at the same cloud provider).

REs and their vendors should take reasonable steps to support each other in order to achieve resilience goals. REs should endeavour to secure the availability of vendors for testing.

REs may consider scenarios where a vendor is unavailable for a considerable period of time or possibly the total failure of a third party and a forced termination of the service/dependency. REs should also assess whether international events may disrupt the local vendor services (e.g., when a vendor is headquartered or runs substantive business elsewhere, especially in high-risk countries subject to natural disasters or political instability).

Similar to other industries (e.g., composite materials), testing should be repeated with increasing severity past failure. Tests can be tweaked to prolong the disruption period, reduce resource availability further or introduce other variables. REs should know the thresholds beyond which impact tolerances cannot be met.

It is not a regulatory expectation that all scenarios are successfully contained all the time. This is especially the case for scenarios over which the RE has no control, such as CNI.

Testing must not risk jeopardising live systems and services. If testing involves live systems or is the appropriate way to realistically test, an RE should assess the risks prior to deciding whether to proceed with the planned test or consider an alternative method of testing. This risk assessment should be retained as part of the testing iteration.

Testing outcomes should feed into several areas that include the following:

a) An increased focus on recovery and response arrangements. This, in turn, may be sub-divided into improving technical controls, bolstering underlying resources (refer to section 7. "Mapping of Resources") and improving communication (refer to section 10. "Communication Plans");

b) Management Information (MI) to the Board and Senior management to aid prioritisation and investment decisions; and

c) Updating and disseminating lessons learned.

10.3 Remediation

The Code sets out the remediation regulatory expectations. REs must take a responsible and sensible approach to remediate any issues that would cause important services to exceed impact tolerances in a real-life, severe, disruptive event.

Responsible and sensible approaches include but are not limited to:

a) Ensuring tests are realistic and as accurate as possible;

b) Taking test results seriously. This goes beyond conducting a 'box-ticking exercise' to comply with regulations;

c) Acting in a timely manner to rectify failures and shortcomings. Remedial action should also be time bound;

d) Investing in resilience. Op Res should be part of the organisational culture and be cascaded down from the top;

e) Prioritising those services that are furthest outside the impact tolerance, where possible, as these are deemed to be the highest-risk services;

f) Taking into consideration possible repercussions for the wider financial sector, contagion and policyholders (in the case of insurers); and

g) Ensuring that remedial action is fit for purpose and caters for complex services, group arrangements and overseas provision of services.

11. Lessons Learned

Embedding operational resilience within an RE and the services it provides is not a one-off exercise. Op Res comprises a set of dynamic activities, including assessment, testing, and integrating the lessons learned back into the RE's operations as part of a continuous cycle of improvement. This should be part of the firm's overall culture and approach.

REs should have clear processes, procedures and management information on their important business services, impact tolerances, possible severe but plausible disruptive scenarios and their ability to remain within tolerance after the first iteration of implementation. The expectation is that REs continue to refine, add to, and fine-tune every aspect of Op Res year-on-year in order to strengthen their own resilience and that of the wider financial sector within Bermuda.

The most valuable lessons can be learned not from simulated testing but by evaluating and reviewing the performance and behaviour of the organisation and its services in the aftermath of real-world disruptive events. These provide the opportunity for an RE to assess whether or not the service remained within tolerance, whether the testing was credible and accurate and whether the scope covered all the variables and resources necessary. Overall, regular Op Res testing is an opportunity to recalibrate and re-run prior tests, improve resilience where it matters most and assess what can be further improved upon. This assessment should include, for example, questions such as these below:

a) Was the disruptive scenario that occurred previously identified as a possibility, or was it not even featured in the testing?

b) Were key people available?

c) Did the disruption highlight any gaps among BAU operations and key personnel in the event of an emergency? Were resources stretched?

d) Would the outcome be different or worse if the disruption had lasted longer?

e) Were there any chain reaction effects that occurred in real life, but were not considered during testing?

f) Were new bottlenecks in resources identified? For example, did the main means of internal communication that is vital to co-ordinating the response become unavailable too?

g) Did third parties, including vendors, utility companies and emergency services, if applicable, behave and react as expected?

h) Was the reaction and mitigation timely?

REs should undertake their own post-mortem self-assessment, using questions applicable to their specific business, size, complexity, and services offered to determine the lessons learned.

12. Self-Assessments and Returns

To demonstrate compliance with the Code, REs are required to document their resilience-related activities and outcomes, prepare a self-assessment annually, and submit the self-assessment to the BMA upon request.

Self-assessments should demonstrate the board's confidence that the RE is able to provide important business services within the RE's impact tolerance year over year. The board is held accountable for Op Res and is responsible for reviewing and approving the self-assessment.

The expected contents of the self-assessment are listed in the Code. The creation of a self-assessment and its submission to the Authority upon request are regulatory requirements. However, the self-assessment should also serve as one of the sources of Op Res MI for the board and senior management, and its level of detail should reflect the complexity, size and nature of the services provided. The self-assessment ties the components of the Op Res lifecycle together and helps rationalise how services are identified, resources mapped, and vulnerabilities captured. Most importantly, the self-assessment should document the efforts and investment the RE is making to improve resilience.

For important business services that are outside impact tolerance thresholds, the self-assessment must describe the actions the RE is planning/undertaking to bring the services within the impact tolerance and the timelines for completion.

13. Appendix A – Definitions

Critical activity - An operational function that is considered critical or important if a flaw or failure in its performance would significantly affect an RE's ongoing compliance with the terms and obligations of its license or registration, other duties under its associated Act, and, or customers and dependent third parties. Such a defect could also have a material impact on the financial performance, stability, or continuity of its operations and activities.

Important Business Service - A service that an RE provides to external consumers to deliver a specific outcome. Important business services are defined as follows if they are disrupted:

- They can cause unacceptable 'harm' to consumers, in particular depositors and policyholders
- They can cause unacceptable 'harm' to other stakeholders
- They pose a contagion risk to Bermuda's financial stability

Material outsourcing - An outsourcing arrangement where a critical activity, as determined by senior management of the RE, has been outsourced to a third party.

Outsourcing - An arrangement in which the RE uses a third-party, i.e., (the outsourcing service provider), to perform activities on an ongoing basis that are integral to the provision of services by the RE itself that would otherwise be undertaken by that RE.

Outsourcing agreement - A written, legally enforceable agreement that sets out contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement. This term also covers performance agreements as set out in the SLAs between the contracting parties.

Outsourcing service provider - A third-party that provides a service to an RE. This third-party entity may or may not be licenced and may be either an affiliated entity within the RE's own corporate group or an entity external to the RE's group.

Sub-contracting/sub-outsourcing/chain outsourcing - An arrangement where the outsourcing service provider that has an outsourcing arrangement with an RE to perform an activity, then sub-contracts the provision of all or part of that activity to other service providers.

14. Appendix B – Glossary of Terms

BCP – Business Continuity Planning
BAU - Business as Usual
DRP – Disaster Recovery Planning
CNI – Critical National Infrastructure
Code – Operational Resilience and Outsourcing Code
MI – Management Information
MTPD – Maximum Tolerable Period of Disruption
PLA – Performance Level Agreement
RE – Relevant Entity – an entity licenced by the Authority under relevant acts
RTO – Recovery Time Objective
RPO – Recovery Point Objective
SLA – Service Level Agreement