Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

Statement of Guidance Statement of GuidanceStatement of Guidance Statement of Guidance Business Continuity Management All Licensees 1. Statement of Objectives 1.1. To enhance the resilience of the financial sector and to minimise the potential impact of a major operational disruption. 1.2. To provide a framework for licensees to develop, implement and maintain their business continuity plans. 2. Introduction 2.1. Business continuity management is a whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption. 2.2. Comprehensive business continuity management addresses not only technical considerations, such as systems and facilities, but also the human dimension, recognising that employees and possibly their families will be affected by the same event that gives rise to business continuity concerns. The personal safety of staff should be the paramount consideration of a licensees business continuity plan. 2.3. Within the financial services sector, there is a sub-set of licensees that provide critical domestic financial services. These include retail banks and insurance licensees that conduct domestic insurance business. These licensees, being aware of their role in the domestic financial market, should ensure a high degree of resilience in the event of a disruption.

Nonetheless, a licensee s business continuity management should be proportionate to its business risk and tailored to the scale and scope of its operations. 3. Business Continuity Planning Process 3.1. Licensees should adopt a process-oriented approach to business continuity planning that involves a. business impact analysis (BIA); b. risk assessment; c. risk management; d. risk monitoring and review. 3.2. A business impact analysis involves the identification of potential impacts of uncontrolled, non-specific events on the licensee s business processes and its customers. The BIA identifies those components of the business that are vulnerable, yet most critical to the continued functioning of the business in the event of a disruption. While every component of a licensee s business is dependent on the smooth functioning of another, the BIA identifies what components are most critical so that resources could be appropriately allocated in the event of a disruption. In identifying critical needs, the licensee should review all functions, processes and personnel within each component of the business. The BIA helps to identify the degree of potential loss that could occur. 3.3. In the risk assessment stage, the business processes and the BIA are stress tested with various threat scenarios. The risk assessment should consider a. the impact of various business disruption scenarios on the licensee and its customers; b. the probability of occurrence based, for example, on a rating system of high, medium, or low;

c. the loss impact on information systems, personnel, facilities, and service providers from both internal and external sources; d. the safety of critical processing documents and vital records; and e. a broad range of possible business disruptions, including natural, technical, and human threats. 3.4. The risk management stage involves the design of risk treatment and the establishment of an enterprise-wide business continuity plan (BCP). Risk treatment is the selection of relevant options for managing risk, including acceptance, avoidance, reduction and transfer of risk. The BCP should be written and disseminated so that various groups of personnel can implement it on a timely basis. It should be specific with respect to the conditions that would prompt the implementation of the plan and with respect to the immediate plans in respect to a disruption. The ultimate objective of the plan is to implement treatments to control risks. 3.5. Risk monitoring and review is the final step in business continuity planning. It should ensure that the licensee s BCP is viable through a. Periodic testing of the BCP; b. Subjecting the BCP to independent audit and review; and c. Updating the BCP upon changes to the internal and external environments. 4. Board and Senior Management Responsibility 4.1. Licensees should have effective and comprehensive approaches to business continuity management. A licensee s board of directors and senior management are collectively responsible for the licensee s business continuity. 4.2. A licensee s board and senior management are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to, and continuity in the event of,

---

operational disruptions. The board and senior management should create and promote an organisational culture that places a high priority on business continuity. This message should be reinforced by providing sufficient financial and human resources to implement and support the organisation s approach to business continuity management. 4.3. A framework should be implemented for reporting to the board and senior management on matters related to business continuity, including implementation status, incident reports, testing results and related action plans for strengthening an organisation s resilience or ability to recover specific operations. A licensee s business continuity management should be subject to review by an independent party, such as internal or external audit, and significant findings should be brought to the attention of the board and senior management on a timely basis. 4.4. Confusion can be a major obstacle to an effective response to an operational disruption. Accordingly, roles, responsibilities and authority to act, as well as succession plans, should be clearly articulated in a licensee s business continuity management policies. Senior management should recognise that they may need to re-align priorities and resources during a disruption in order to expedite recovery and respond decisively. It is important that a locus of responsibility for managing business continuity during a disruption is established, such as a crisis management team with appropriate senior management membership. In addition, senior management should be involved in communicating the licensee s response, commensurate with the severity of the disruption. 5. Major Operational Disruptions 5.1. Major operational disruptions pose a substantial risk to the continued operation of the financial sector. Accordingly, licensees should incorporate the risk of a major operational disruption in their business continuity plans. The extent to which a licensee prepares to recover from a major operational disruption should be based on its unique characteristics and risk profile.

Hurricane Ivan demonstrated in 2004 some of the operational challenges that licensees could face on the low-lying island of Grand Cayman: - staff accommodation damaged or destroyed; - roads not immediately passable due to damage, debris, or flooding; - significant numbers of cars damaged by flood; - generators placed at ground level flooded; - severe disruption to electricity and telecommunication systems; - airlines chartered to evacuate staff, but licensees unable to obtain visas on time.

5.2. Because access to the resources needed for the full recovery of its operations may be limited during a major operational disruption, licensees should a. identify through a business impact analysis those business functions and operations that are to be recovered on a priority basis; and b. establish appropriate recovery objectives for those operations.

5.3. Major operational disruptions vary in intensity and scope. In many cases, licensees may be able to remain at their primary business locations if they have sufficient backup for power and other essential services. Experience, however, has demonstrated that some major operational disruptions constitute extreme events whose impact can be very broad. In evaluating whether their own business continuity management is sufficient to accommodate such major operational disruptions, licensees should review the adequacy of their recovery arrangements in three important areas: a. First, a licensee should take care that its alternate site is more resilient and/or sufficiently remote from its primary business location. This minimises the risk that both could be affected by

the same event. For example, the alternate site could be a purpose-built disaster recovery centre in the area, or a building located on a sister island or overseas (in the case of licensees conducting international business). For the maintenance of records outside the Cayman Islands, note section 5 of the statement of guidance on Nature, Accessibility and Retention of Records. b. Second, a licensee should consider whether the alternate site would have sufficient current data and the necessary equipment and systems to recover and maintain critical operations and services for a sufficient period of time in the event that its primary offices are severely damaged or access to the affected area is restricted. For storage of data outside the Cayman Islands, licensees are encouraged to arrange for storage in jurisdictions approved by the Authority and may look to establish real time replication capabilities. c. Third, given that staff may be impeded from returning to the primary place of business or may simply be unavailable, the business continuity plan should address how the licensee will provide sufficient staff in terms of number and expertise to recover critical operations and services consistent with its recovery objectives. Some approaches to ensuring that sufficient staff are available at alternate sites include: i. temporarily relocating staff at alternate sites as the need arises; ii. placing staff at alternate sites on a permanent basis (e.g. in the case of load-sharing); and iii. cross-training employees at alternate sites or from other locations, ensuring that a percentage of employees deemed essential to meeting recovery objectives are

located away from the primary business location at any given time. 6. Recovery Objectives 6.1. A licensee that experiences a major operational disruption might affect the ability of other financial sector participants and possibly the domestic financial system to continue normal business operations. Accordingly, licensees should consider the extent to which they pose such a risk and augment their business continuity management where they determine that a disruption of their operations would affect the operation of the broader domestic financial system. 6.2. Licensees should establish recovery objectives that are proportionate to the risk they pose to the operation of the domestic financial system. The responsibility for setting recovery objectives rests with the licensee s board and senior management. The highest recovery objectives typically should be reserved for those licenses that are most likely to disrupt the domestic financial system in the event of a major operational disruption because of the critical services they provide or their significance to the financial system in which they operate. For example, critical market participants might reasonably be held to a five-day recovery time objective, and expected not only to recover critical operations and services but also to resume new business within the same timeframe. It may be acceptable for other participants to target a less stringent recovery time depending on the impact a disruption of their operations would have on the financial system or on the expectations of other licensees. 6.3. In assessing the reasonableness of an organisation s recovery objectives, the Authority will consider the increased risk of failed transactions, liquidity dislocations, solvency problems, and loss of confidence that accompany prolonged disruptions in the financial system. 6.4. Recovery objectives should identify expected recovery levels and recovery times for specific activities. Although they may not be achievable in every

circumstance, recovery objectives provide licensees with benchmarks for testing the effectiveness of their business continuity management. They also provide some assurance that financial sector participants representing similar external risks will attain a consistent level of resilience. When identifying recovery objectives, it would also be appropriate to identify appropriate timeframes for implementing those objectives. 7. Communications 7.1. Licensees should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties, such as their associations and the Authority, in the event of a major operational disruption. 7.2. The ability to communicate effectively with relevant internal and external parties in the event of a major operational disruption is essential, particularly in the early stages of a disruption. Effective communication is necessary to gauge the impact of the disruption on a licensee s staff and operations, and on the broader financial system and make appropriate decisions about whether to invoke the BCP. As time progresses, the ability to communicate the best available information to the appropriate parties in a timely fashion is critical to the recovery of an organisation s operations and to the return of the broader financial system to normal operation. Maintaining public confidence, whether in an individual business or in the financial sector as a whole, requires clear, regular communication throughout the duration of a major operational disruption. 7.3. Because of the added pressure that is often associated with decision-making during a major operational disruption, the BCPs of licensees should incorporate comprehensive emergency communication protocols and procedures. For example, a licensee would need to consider how best to communicate within the organisation as well as with its association, the Authority, other licensees, the public and other stakeholders.

7.4. Information collected by the Authority from licensees and the relevant associations will be processed and utilised on a consolidated basis when issuing public statements during a crisis. Information received by the Authority may also be used as part of an overall national economic impact assessment exercise. 7.5. The communication procedures of licensees generally should: a. Identify those responsible for communicating with staff and various external stakeholders. This group might include senior management, public affairs staff, legal and compliance advisors, and staff responsible for the organisation s business continuity procedures. This group should be able to communicate with personnel located at isolated sites, dispersed across multiple locations, or otherwise away from the primary business location; b. Build on any communication protocols that already exist within the financial system and include contact information for the Authority, industry associations and other relevant participants to facilitate an assessment of the condition of the financial system and coordinate recovery efforts. In addition, consideration should be given to including contact information for officials with local emergency response organisations where critical facilities are located; c. Address related issues that can arise during a major operational disruption, such as how to respond to failures in primary communication systems. This could include, for example, developing systems and contact information for key personnel that would facilitate multiple methods of communicating (e.g. digital and analogue land line phones, mobile phones, satellite phones, text messaging, websites, hand-held wireless devices, etc); and d. Provide for the regular updating of calling trees and other contact information and the periodic testing of calling trees.

---

8. Outsourcing 8.1. Licensees should recognise that outsourcing a business operation does not transfer the associated business continuity management responsibilities to the vendor. Where a significant business activity is outsourced, there should be a contingency plan in place in the event that such arrangement is terminated or the vendor is unable to fulfil his obligation. Also, outsourcing agreements should address business continuity plans so that both the licensee and the vendor know what to expect in the event of a disruption. 9. Training 9.1. Licensees should provide business continuity training for personnel to ensure all parties are aware of their responsibilities in the event of a disruption. Key employees should be involved in the business continuity development process, as well as periodic training exercises. The training programme should incorporate enterprise-wide training as well as specific training for individual business units. Employees should be aware of which conditions call for

implementing all or parts of the BCP, who is responsible for implementing BCPs for business units and the institution, and what to do if these key employees are not available at the time of a disaster. Cross training should be utilised to anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the BCP. 10. Testing L:\Adition\IT Division\Projects\Website\Content\Updates\SOG\SOG_Internal_Audit_ 10.1. Licensees should test their business continuity plans, evaluate their effectiveness, and update their business continuity management as appropriate. 10.2. Testing of the ability to recover critical operations, as intended is an essential component of effective business continuity management. Such

testing should be conducted periodically, with the scope and frequency determined by the criticality of the applications and business functions, the organisation s role in broader market operations, and material changes in the organisation s business or external environment. In addition, such testing should identify the need to modify the business continuity plan and other aspects of an organisation s business continuity management in response to changes in its business, responsibilities, systems, software, hardware, personnel, or facilities or the external environment. An independent party, such as internal or external audit, should assess the effectiveness of the organisation s testing programme, review test results and report their findings to senior management and the board. 10.3. In addition to ensuring that business continuity plans are evaluated and updated on an ongoing basis, testing is also essential for promoting awareness, familiarity and understanding among key personnel of their roles and responsibilities in the event of a major operational disruption. It is important, therefore, that testing programmes should involve all personnel who are likely to be involved in responding to major operational disruptions. 11. Business Continuity Review by the Authority 11.1. The Authority incorporates business continuity management reviews into its examination/inspection procedures. 11.2. The Authority expects licensees to develop and implement effective business continuity management that is updated on an ongoing basis. Examination/inspection procedures will give due consideration to whether a licensee s business continuity management, including its recovery objectives, is appropriate for the size and scope of its business and the risk the licensee presents to the continued operation of the financial system. The Authority will also assess whether licensees are taking appropriate steps to augment their business continuity management, and whether the

testing programme provides adequate assurance that business processes can be recovered as intended. 12. The General Guidance 12.1. This Statement of Guidance has been adapted from the Basel Committee on Banking Supervision Joint Forum on High Level Principles for Business Continuity, December 2005, and the Business Continuity Planning IT Examination Handbook of the Federal Financial Institutions Examination Council, March 2003.