INDUSTRY-WIDE SURVEY ON BUSINESS CONTINUITY MANAGEMENT

SUMMARY OF FINDINGS

MAS Information Paper
December 2013
PREFACE

Business continuity management ("BCM") is an important part of financial institutions’ ("institutions") risk management. It contributes to the operational resilience of both institutions themselves and Singapore as a financial centre. A well-implemented BCM programme ensures the continuity of critical activities in the event of major operational disruptions.

MAS has provided various BCM guidance to institutions over the years. In June 2003, MAS published its first BCM Guidelines ("the Guidelines"). In 2006, a circular was issued to institutions to provide further guidance on pandemic and security measures. This was followed up with an information paper on preparedness for avian influenza pandemic and security threats, presenting sound practices adopted by key institutions, as observed through MAS’ supervision of institutions. In order to promote resilience and preparedness, MAS also co-organises industry-wide BCM exercises and is engaged in industry BCM working groups that discuss various issues.

This information paper summarises findings from the Industry-wide BCM Survey ("the survey"), which MAS conducted from May to July 2012. MAS hopes that the findings provide useful insights into the current state of BCM in institutions, and facilitate benchmarking of BCM practices among institutions. Where applicable, institutions can adopt the good practices highlighted, as well as move to address potential gaps.

Should you have any questions or comments, please contact Terry Goh, Director, Specialist Risk Department at 62299811 or terrygoh@mas.gov.sg.

Ho Hern Shin
Head of Specialist Risk Department
December 2013
TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY .................................................................1

2.0 INTRODUCTION ............................................................................3

  2.1 Background ................................................................................3

3.0 OVERVIEW OF BCM LANDSCAPE .............................................3

  3.1 Overall state of BCM implementation in the financial industry ....3
  3.2 Risk-appropriate BCM practices ..............................................4

4.0 FINDINGS ON SPECIFIC BCM PRACTICES ...............................4

  4.1 Governance – Senior management responsibility for BCM is entrenched although adoption of BCM attestation should be greater .................4
  4.2 Risk assessment – A holistic approach to assess threats and corresponding mitigating controls should be taken. ..................5
  4.3 Business Impact Analysis (“BIA”) – The BIA should be conducted for all business functions. ...........................................5
  4.4 Business continuity planning – There should be greater adoption of staff loss as a planning assumption. .........................6
  4.5 Recovery objectives – Recovery Time Objectives (“RTO”) should commence from the point of disruption ......................6
  4.6 Recovery strategies – Most institutions have planned for prolonged operations from an alternate location. .......................7
  4.7 Crisis management and communications – Core components are well-established. .................................................7
  4.8 Training and awareness - Institutions should establish a formal training and awareness programme. .............................8
  4.9 Testing - There should be greater adoption of more challenging test objectives ..............................................................8
  4.10 Physical security threats – There should be greater adoption of a security framework and increased participation in public-private partnerships programmes ..........9
  4.11 Pandemic planning – Pandemic response plans are largely present. More institutions should establish a quarantine and contact tracing framework .......................9

5.0 CONCLUSION ..............................................................................10
1.0 EXECUTIVE SUMMARY

1.1 This information paper presents a summary of findings from the 2012 Industry-wide Business Continuity Management (“BCM”) Survey (“the survey”). The survey was conducted to form an overview of the current landscape of BCM practices across financial institutions (“institutions”) and to identify key areas for improvement. 371 responses were received from approved exchanges, banks, capital market services (“CMS”) licensees, finance companies, insurers and reinsurers.

1.2 The findings related to the general state of BCM are as follows:

- Overall, there is a widespread adoption of BCM practices in the financial industry. Most respondents have put in place a BCM programme. Most also incorporate core components of BCM in their BCM framework.

  BCM maturity varies across categories of respondents. Key institutions show a higher level of BCM maturity through the adoption of more robust BCM practices and methodologies. Adoption of the core BCM components and sufficiently detailed crisis management plans are also more consistently observed amongst approved exchanges, banks and finance companies compared to other categories of institutions.

1.3 While the presence of BCM and its core components in most respondents indicate a positive overall landscape, the survey also highlighted some opportunities for improvements:

  a) Adopt a formal process for BCM attestation by senior management (Section 4.1)
  b) Extend the Business Impact Analysis (“BIA”) to cover all functions (Section 4.3)
  c) Align Recovery Time Objectives (“RTOs”) definition across business and information technology (“IT”) functions, and have RTOs commence from the point of disruption (Section 4.5);

---

Core components identified are the BCM risk assessment, business impact analysis, business continuity plans, crisis management plans and testing.
d) Establish BCM training and awareness programmes (Section 4.8); and
e) Adopt more challenging test objectives (Section 4.9)

1.4 MAS would like to extend its appreciation to all respondents.
2.0 INTRODUCTION

2.1 Background

2.1.1 The Monetary Authority of Singapore 2012 BCM survey sought to provide an overview of the prevailing landscape of BCM practices across institutions and to identify areas for improvement. As such, it was comprehensive in scope and depth, with detailed questions on key aspects of BCM. The questions covered institutions’ BCM practices across 10 categories – governance, risk assessment, Business Impact Analysis (“BIA”), business continuity planning, identification & prioritisation of critical business functions (“CBFs”), training & awareness, crisis management & communications, recovery objectives & strategies, testing and physical security & pandemic threats. Responses from 371 institutions, including approved exchanges, banks, CMS licensees, finance companies, insurers and reinsurers were received. Please see Table 2.1 for the respondent profile.

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks and finance companies</td>
<td>151</td>
</tr>
<tr>
<td>Insurers and reinsurers</td>
<td>62</td>
</tr>
<tr>
<td>CMS licensees and approved exchanges</td>
<td>158</td>
</tr>
<tr>
<td><strong>Total respondents</strong></td>
<td><strong>371</strong></td>
</tr>
</tbody>
</table>

3.0 OVERVIEW OF BCM LANDSCAPE

3.1 Overall state of BCM implementation in the financial industry

3.1.1 Results from the survey show that the importance of having business continuity preparedness seems well accepted in the financial industry. This is reflected in the widespread adoption of fundamental BCM practices across the industry. Most respondents have in place a BCM programme and have adopted the core components of BCM in their BCM framework.

---

2 These are functions of high importance that the institution should maintain to ensure its reputation and survivability. Critical business functions differ among institutions largely due to different business focus and customers’ expectations. Some critical business functions would include: completing payment instructions, clearing and settling transactions, fulfilling end-of-day funding and collateral obligations, managing customers’ risk positions and maintaining customer, investor or public confidence.

3 The core components identified are the BCM risk assessment, Business Impact Analysis, business continuity plans, crisis management plans and testing.
3.1.2 Respondents from banks, finance companies and approved exchanges demonstrate a higher level of BCM maturity as compared to insurers, reinsurers and CMS licensees. This is evidenced by a higher level of adoption of the core BCM components and greater comprehensiveness in the documentation of crisis management plans. There is a greater degree of financial intermediation performed by these institutions and they tend to have more complex interactions with a larger community of stakeholders. These can lead to higher client and stakeholder expectations and stronger emphasis placed by these institutions on organisational resilience. Hence, the need to more comprehensively address BCM issues.

3.1.3 Respondents from key institutions also tend to be more mature in the implementation of the BCM framework, as compared to other institutions. This is reflected in their more robust BCM practices and methodologies.

3.2 Risk-appropriate BCM Practices

3.2.1 Ultimately, institutions should continue to adopt the appropriate measures and implement a BCM programme that is commensurate with the nature, scale and complexity of their business activities. A well implemented risk-appropriate BCM programme will best assure an institution of its ability to continue with its CBFs and enable it to fulfil business obligations in the event of operational disruptions.

4.0 FINDINGS ON SPECIFIC BCM PRACTICES

4.1 Governance – Senior management responsibility for BCM is entrenched although adoption of BCM attestation should be greater.

4.1.1 Senior management plays an important role in steering an institution’s BCM programme. Most respondents indicated that senior management assumes ultimate responsibility for the institution’s business continuity preparedness. This represents a recognition of senior management’s role in steering BCM, and active efforts made by institutions in engaging them on BCM matters.

4.1.2 Senior management attestation provides assurance to stakeholders on the effectiveness of the institution’s BCM programme. While most respondents indicated that they have a formal BCM attestation process, a few respondents do not have such a process. In place of a formal senior management attestation,
some respondents involved their senior management in BCM discussions at various management forums as a substitute for such attestation.

4.1.3 An attestation should be a formal process where senior management explicitly attests to the business continuity preparedness of the institution. The attestation should also contain sufficient details to provide the needed assurance.

4.2 Risk assessment – A holistic approach to assess threats and corresponding mitigating controls should be taken.

4.2.1 Risk assessment of the institution’s operating landscape is an important component of the BCM programme. It provides institutions with a comprehensive view of its risk landscape and defines the focus of the BCM programme. Most respondents identify internal and external threats, such as physical and cyber attacks in their risk assessments. However, a number of institutions do not go on to assess the corresponding mitigating controls for these identified threats, such as physical hardening of facilities and implementing firewalls. Institutions should adopt such a holistic approach, which incorporates both threats and controls assessments, to facilitate clearer identification of any residual risks.

4.3 Business Impact Analysis (“BIA”) – The BIA should be conducted for all business functions.

4.3.1 In the event of a disruption, it might not be practical for an institution to recover all business functions at the same time. A BIA allows an institution to assess the various legal, financial, reputational and other impacts that could result from a disruption of the business function. This facilitates institutions in identifying and prioritising business functions that are most critical to recover quickly in an outage.

4.3.2 Most respondents from key institutions conduct the BIA for all business functions. However, there are some institutions that either do not conduct the BIA, or only conduct the BIA for some functions. Some respondents also adopt a ‘fast-track’ approach to their BIA process. This involves using management judgement to pre-determine CBFs and conducting the BIA only for these functions to validate that these functions are deemed critical.

4.3.3 The BIA should be fundamentally applied to all functions. This would enable institutions to accurately and comprehensively identify the impact arising...
from the operational disruption of each business unit. This in turn ensures that the CBFs can be appropriately prioritised and corresponding RTOs determined.

4.4 Business continuity planning – There should be greater adoption of staff loss as a planning assumption.

4.4.1 Planning assumptions help to adequately scope institutions’ response and recovery plans. While the loss of IT and denial of access to premises are common BCM planning assumptions amongst most respondents, loss of staff as a key planning assumption is adopted more commonly only amongst key financial institutions. Staff loss could result from a sudden, high impact scenario such as a building attack or a slow-burn scenario such as a pandemic outbreak. Given the significant impact staff loss could have on an institution’s business continuity efforts, it should be used as a BCM planning assumption by institutions.

4.5 Recovery objectives – Recovery Time Objectives (“RTO”) should commence from the point of disruption.

4.5.1 The RTO is a key planning parameter, both for institutions and their stakeholders. It is a measure of how quickly a particular business function, and by extension, the institution seeks to recover following a disruption. It is likely to feature prominently in service level agreements to ensure that externally provided services are also able to meet the institution’s recovery objectives. As such, it is important to establish a clear and common understanding of the RTO definition. Many respondents from key institutions define the RTO to start from the point of disruption. However, across all respondents, some institutions define RTO to start from the point of activation of the business continuity plan (“BCP”) instead.

4.5.2 To align with the Guidelines⁴, institutions should define the RTO to commence from the point of disruption. Further, this definition should be similarly applied across business and IT functions. Given the high degree of reliance on IT by institutions, alignment in RTO definitions will help to ensure that IT functions are able to recover quickly enough to meet business needs.

⁴ The MAS BCM Guidelines define RTO as the target duration of time to recover a specific business function. It comprises two components: (1) The duration of time from the point of disruption, to the point of declaring the activation of BCP, and (2) The duration of time from the activation of the BCP to the point when the specific business function is recovered. It is the acceptable duration of time that can elapse before the non-continuation of the specific business function would result in severe business impact and losses to the institution.
4.6 Recovery strategies – Most institutions have planned for prolonged operations from an alternate location.

4.6.1 Recovery strategies enable institutions to minimise disruption and potential losses. They define the key steps to take following a disruption and help to achieve an orderly and timely execution of BCPs. It is encouraging to note that most respondents have strategies to operate from business recovery sites during a prolonged outage. Many respondents also intend to deploy staff to work from home or transfer relevant critical functions overseas. An effective combination of such strategies helps to build resilience within an institution. It also instils confidence in its stakeholders and helps to preserve the institution’s reputation.

4.6.2 While some institutions utilise business continuity service providers to provide business recovery sites, the majority of institutions have developed in-house capacity for such premises. Work-from-home strategies further extends a conventional business-as-usual operation model to a viable BCM strategy for most institutions. The strategy of transferring relevant critical functions overseas are adopted by many multinationals that have integrated cross-border operations. However, there are important considerations in implementing such strategies, such as logistical as and regulatory factors, among others. Ultimately, institutions should decide on the strategies which best enable them to meet their business obligations.

4.7 Crisis management and communications – Core components are well-established.

4.7.1 Crisis management and communications facilitate the understanding of the disruption and the dissemination of information to stakeholders. Effective crisis management provides material information to the appropriate parties and allows senior management make informed decisions. Most respondents include the roles and responsibilities of the crisis management team members, escalation procedures, and emergency response procedures in their crisis management plan.

4.7.2 In the area of crisis communications, mobile phones and email are the main channels preferred by most respondents. In addition, most key institutions indicated that they use the institution’s internet portal for crisis communications. Some respondents from key institutions also use grid phones, with a few also using satellite and voice over internet protocol phones. While most institutions
use a variety of channels for crisis communications, others still rely on channels which they use on a daily basis.

4.7.3 Evolving developments during a crisis will constantly challenge crisis management and communications. Having well-developed crisis management plans that facilitate quick and timely decision-making in a crisis will benefit institutions. Alternative channels of communication should also enhance the dissemination of information.

4.8 Training and awareness - Institutions should establish a formal training and awareness programme.

4.8.1 A well-structured training and awareness programme will provide all personnel with the requisite knowledge to prepare for any operational disruption and to carry out their BCM roles more effectively and efficiently. It is also important to have a specialised training programme for staff that have BCM responsibilities, such as senior management and BCM personnel. In addition, a general awareness programme can also provide staff with an appreciation of actions that they should take in the event of a disruption. Most respondents have both training and awareness programmes in place. Training is mostly carried out through avenues such as seminars, while awareness programmes are carried out in the form of regular BCP walkthroughs, briefings, access to shared BCM documents, and participation in BCM tests. However, it is of concern that a number of respondents have yet to put such programmes in place.

4.8.2 The BCM programme applies to all levels of the institution, from senior management and staff with BCM-related roles to general staff. All institutions should evaluate current needs and implement a formal BCM training and awareness programme.

4.9 Testing - There should be greater adoption of more challenging test objectives.

4.9.1 Testing is a vital element for implementing an effective BCM implementation. Evolving changes in technology, business processes, and roles and responsibilities will affect the institutions’ BCPs, which should be validated through testing. The ability to resume operations from alternate business recovery sites and to achieve the RTOs of CBFs are the top test objectives set by most respondents.
4.9.2 In addition, most respondents from key institutions conduct end-to-end testing to validate the recoverability of front, middle and back office functions in tandem. Many also validate RTOs across the institution. These are more challenging objectives that contribute to complete and meaningful testing of an institution’s BCM. As such, they should be more widely adopted.

4.10 **Physical security threats** – There should be greater adoption of a security framework and increased participation in public-private partnerships programmes.

4.10.1 Physical security threats can materialise and affect the businesses of an institution. While most respondents have established a physical security threat and response framework, a few respondents have not done so. This may indicate a reliance on the institutions’ building management security framework for the entire building premise. Such frameworks are typically broad-based and do not address institution-specific security needs. Institutions should develop an internal framework to address security threats and response in the context of their operations.

4.10.2 Most respondents from key institutions currently participate in various public-private partnership schemes, such as the Safety and Security Watch Group\(^5\). Many also sign up for the Corporate First Responder scheme\(^6\). These schemes represent areas in which institutions can engage more actively to facilitate institutional response in a disruption, in collaboration with the public authorities. They also offer a channel for institutions to interface with the authorities to discuss relevant issues prior to disruptions and to facilitate institutions to network and share best practices. As such, more institutions should participate in such public-private partnership schemes.

4.11 **Pandemic planning** – Pandemic response plans are largely present. More institutions should establish a quarantine and contact tracing framework.

4.11.1 Institutions should take measures to mitigate the impact of a pandemic, which can result in low staff availability and potentially disrupt business

---

\(^5\) The Safety and Security Watch Group scheme groups buildings according to geographical clusters. It allows buildings to work together with public authorities on physical security issues such as local threat assessment and security enhancement.

\(^6\) The Corporate First Responder scheme allows building management and tenants to identify key personnel who will be allowed into the cordoned area in the aftermath of a major incident to assist with rescue, recovery and investigation efforts, as well as carry out business continuity activity.
operations for prolonged periods. Most respondents have catered for the implementation of pandemic response plans as part of their BCM programme. The high degree of adoption could be due to the Industry-wide Exercise 2008, which was based on an avian influenza scenario, and a general increase in awareness from real life episodes, such as SARS, avian influenza, and Influenza A – H1N1 (2009).

4.11.2 However, only a significantly lower portion of respondents indicated that they have a framework for quarantine and contact tracing. Such a framework is a fundamental component of a pandemic plan and should be established by all institutions.

5.0 CONCLUSION

5.1 The industry-wide BCM survey has provided a useful view of the current state of BCM in institutions by identifying key trends and areas for improvement. MAS hopes that this information paper will serve as a useful reference for institutions on assessing their BCM programmes. We would like to extend our appreciation to all institutions that have responded to the survey.