AUTORITÉ
DES MARCHÉS
FINANCIERS

BUSINESS CONTINUITY MANAGEMENT GUIDELINE

April 2010

Contents

Introduction

The financial sector is composed of a multitude of interconnections between various marketplaces, systems, participants and service providers. A disruption, slowdown or interruption in the activities of a financial institution or any of its service providers, due to operational issues, could jeopardize its ability to honour its commitments to its clients and partners and, in certain cases, disrupt the financial system through a trickle-down effect. Given these interdependencies and the complex functioning of the financial sector, financial institutions should adopt sound and prudent management practices to ensure business continuity in the event of an operational incident. Business continuity management is a priority in the sound management of operational risk.

Business continuity management consists in establishing procedures to identify major operational incidents likely to pose a threat to the financial institution, such as natural disasters, power outages, telecommunications failures, computer malfunctions, piracy, terrorism, pandemics and the like. By identifying these events, the institution can assess their impact on its operations and implement the necessary mitigation measures to ensure the continuity of critical business activities.

This guideline sets out the expectations of the AMF regarding business continuity management. Under the various sector-based laws it administers,[1] the AMF has the authority to establish guidelines regarding sound and prudent management practices for financial institutions.

The principles of business continuity management proposed by the AMF are based on the frame of reference[2] adopted by Québec's *Ministère de la Sécurité publique*, which proposes a collective approach to ensure consistency and complementarity in the management of business continuity. This approach requires the involvement of government authorities, health agencies and all other organizations and institutions that provide essential products or services.

This guideline is also based on the core principles published by the Basel Committee on Banking Supervision[3], the International Association of Insurance Supervisors[4] and the Joint Forum[5] with respect to sound operational risk management practices and sound business continuity management practices.

1 *Insurers Act*, CQLR, c. A-32.1, section 463; *Deposit institution and deposit protection act*, CQLR, c. I-13.2.2, section 42.2; *Act respecting financial services cooperatives*, CQLR, c. C-67.3, s. 565.1. *Trust companies and savings companies Act*, CQLR, c. S-29.02, section 254.

2 Gouvernement du Québec, Ministère de la Sécurité publique, *Gestion des risques en sécurité civile*, 2008; *Approche et principes en sécurité civile*, 2008.

3 Basel Committee on Banking Supervision, Bank for International Settlements. *Sound Practices for the Management and Supervision of Operational Risk*, February 2003.

4 International Association of Insurance Supervisors, *Insurance Core Principles and Methodology*, October 2003.

5 Joint Forum, *High-level principles for business continuity*, August 2006.

1. Continuity and resumption of business

For purposes of this guideline, business continuity management is defined as a process resulting from a strategy and a policy, and procedures intended to ensure the continuity and resumption of a financial institution's critical business activities following an operational incident. An institution's critical functions are those whose disruption, slowdown or interruption over a certain period of time would have a material impact on the financial institution's operations. In addition to the material impact of the incident, the institution's clients and suppliers may likely be affected, with potential unfavourable consequences on the institution's financial position and, ultimately, its reputation.

Operational incidents are events that disrupt, slow down or interrupt an institution's critical functions and result in financial losses or damage to the institution's reputation. Such incidents may be attributable to the institution's own procedures, to its human resources and internal systems or to external events such as natural disasters, fires, power outages, telecommunications failures, computer malfunctions, piracy, malicious attacks, terrorism, pandemics and the like.

With this in mind, each financial institution should adopt a carefully developed business continuity plan ("BCP") to ensure it is optimally prepared to handle major operational incidents. BCP is a written action plan that sets out the procedures and resources required for the continuity and resumption of the institution's operations.

2. Sound and prudent business continuity management

The AMF realizes that an institution will opt for a business continuity management process based on several factors, including its size and the type and complexity of its activities. Regardless of the process adopted, an effective business continuity management process should be based on the principles set forth below, including the clear formulation of a continuity strategy and the participation of senior management and the board of directors.

The business continuity management process should also take into account the nature and scope of the operational incidents identified by the institution. This guideline only applies to major operational incidents. In determining the scope of its continuity management, an institution could rely on a risk-based approach in which the various incidents are evaluated on the basis, among other things, of their probability of occurrence and severity, thereby allowing the institution to establish recovery priorities. Setting priorities depends on the time required to resume operations and the seriousness of the consequences that would result from an interruption of operations. The institution could then determine minimum service levels and acceptable interruption periods. An institution's inability to deliver essential products and services can have a serious impact on its reputation. Business continuity management is an effective way to meet this challenge.

This guideline sets out principles to foster rigorous and effective management of the business continuity of financial institutions based on a systematic and structured approach. These principles are also intended to foster a comprehensive, permanent and integrated approach to the management of a financial institution's risks.

In essence, the principles address the organization of continuity management, the identification of major operational incidents, the assessment of their impact on the institution's critical functions and the planning of continuity management.

3. General framework for business continuity management

Principle 1: Responsibility of senior management and the board of directors

> The AMF expects business continuity management to form an integral part of the financial institution's integrated risk management, for which the board of directors and senior management are ultimately responsible.

The AMF expects the roles and responsibilities related to business continuity management to be clearly defined and adequately documented. The Governance Guideline[6] sets out sound and prudent management principles that a financial institution should consider a priori, in light of the particular nature of business continuity management. In this regard, the board of directors should notably:

- approve the business continuity strategy and policy; and
- appoint a member of senior management to be in charge of business continuity management.

The roles and responsibilities of senior management should include the following:

- ensuring the effectiveness of business continuity management and the resumption of disrupted or interrupted business activities within reasonable time limits;
- creating and promoting an organizational culture that places a high priority on business continuity management;
- approving the BCP;
- becoming involved in the event of major business continuity incidents by adapting pre-established guidelines to unforeseen circumstances;
- ensuring the institution's financial survival;
- periodically submitting reports to the board of directors on the financial institution's ability to respond to an incident; and
- allocating the necessary resources for developing and implementing the BCP.

Senior management should establish a business continuity management committee. This committee could be responsible for drafting, planning, verifying and updating the BCP. It could also be in charge of implementing the BCP, co-ordinating activities and supervising the development of the BCP. In certain cases, a single person in charge of the BCP could be sufficient. However, it would not be necessary to appoint such a person where laws provide for structures or committees that can assume such a task.

Principle 2: Strategy, policy and procedures

> The AMF expects financial institutions to adopt a strategy to ensure the continuity of critical business activities and the resumption of disrupted or interrupted business activities within reasonable time limits.

Business continuity management should form an integral part of the financial institution's day-to-day management. The financial institution should develop a business continuity strategy and implement a

6 Autorité des marchés financiers, *Governance Guideline*.

policy and procedures to execute the strategy at the operational level by addressing the following elements, in particular:

- the creation of a business continuity management committee involving senior management;
- the definition of the roles and responsibilities of all parties who may be involved;
- the establishment of plans for delegating powers so as to respond effectively to unforeseen circumstances and reduce uncertainties as to who assumes responsibility in the event of a disruption, slowdown or interruption affecting the institution's critical functions;
- the identification of major operational incidents likely to affect the financial institution;
- the identification of critical functions;
- the analysis of the impact of major operational incidents on the institution's critical functions;
- the development of business continuity objectives;
- the development of a comprehensive BCP setting out the actions to be taken;
- the co-ordination of the financial institution's actions with the actions of government authorities and/or service providers;
- the implementation of training and awareness program for the employees involved;
- the development of a communication plan; and
- the verification of the reliability of the BCP and the updating thereof.

4. Identification and analysis of major operational incidents

Principle 3: Identification of major operational incidents

> The AMF expects financial institutions to identify the major operational incidents likely to disrupt, slow down or interrupt their critical functions

In addition to the operational incidents that are commonly identified, such as natural disasters, computer malfunctions, terrorist attacks and other intentional or accidental acts, a financial institution may be affected by new events related to growing automation, increased reliance on outsourcing and the interdependencies of the financial system. Certain incidents, such as an influenza pandemic, have a direct impact on human resources, but the majority of operational incidents damage or undermine systems and physical infrastructure.

Major operational incidents can result in one or more of the following consequences: damage to, or destruction of physical infrastructures and systems, unavailability or loss of human resources, limited access to the affected areas, financial losses and injury to an institution's reputation. Any of these incidents can also result in significant financial losses. They can even seriously damage an institution's reputation. Ultimately, they can impact the entire financial system.

A financial institution should therefore identify the incidents likely to affect it and assess their impact on its risk profile. The following are the primary criteria for identifying major operational incidents and setting priorities for managing them:

- intensity;
- likelihood of occurrence;
- the site and geographic scope of the incident;
- propagation speed;
- duration of impact;
- when the disruption is likely to occur;
- predictability; and
- possibility of containing or controlling the incident.

The institution should also consider the fact that the occurrence of certain incidents could trigger secondary incidents. For example, an earthquake could cause fires due to gas leaks.

Principle 4: Identification of critical functions

> The AMF expects a financial institution to identify its critical business continuity functions, their concentration at a single site, their interdependencies as well as their dependence on a single system, staff or service providers.

The financial institution should ensure that the services of the providers on which its critical functions depend will be available. For example, the institution should routinely test the communications systems between its sites and those of its service providers. Similarly, the financial institution should ascertain that the risks related to its outsourced activities do not jeopardize its business continuity. Thus, the institution should

ensure that its service providers have reliable BCPs, and should adapt its own BCP based on the residual risks identified.[7]

In addition, certain financial institutions may have chosen to centralize some of their critical functions and support functions (e.g. electronic data processing). This centralization could increase the risk that the functions located on a given site or dependent on that site will be interrupted in the event of an incident. Accordingly, the financial institution should consider putting into place the necessary measures to mitigate the risks related to the concentration of its business activities. For example, it could set up recovery sites.

Principle 5: Assessment of impact on critical activities

> The AMF expects a financial institution to assess the impact of major incidents on its resources, operations and environment and determine the measures to be taken in light of this assessment.

In assessing the impact of major operational incidents on its critical activities, the financial institution should, in particular, consider the following:

- the effects on the infrastructures, systems and physical resources on which the financial institution depends for its day-to-day operations, such as electrical power, telecommunications, and the like;
- the effects on the population linked geographically and economically with the financial institution (e.g. its staff, clients, suppliers, partners, and the like); and
- the financial and economic consequences.

The financial institution should also consider systemic risk when assessing the impact on its environment. For a number of operational incidents (such as natural disasters, influenza pandemic, etc.), the occurrence of a systemic risk should be taken into account, because such incidents can have a widespread geographical impact. The scope of the impact could be exacerbated by the interconnection of the financial markets and the interdependencies of our economic systems.

In assessing the impact of a major incident, the financial institution should estimate the availability of the resources necessary to pursue each critical activity (human and physical resources, service provider processes, telecommunications networks, etc.). It should also consider the mitigation measures it has in place (e.g., recovery sites, data backup plans, etc.).

The impact assessment should allow the financial institution to anticipate potential disruptions, slowdowns and interruptions affecting its critical activities. Based on this assessment, the financial institution should establish its business continuity and resumption objectives, including:

- managing the immediate consequences of an incident;
- ensuring the continuity of critical activities;
- maintaining an appropriate level of service; and
- reducing the duration of the interruption to a level acceptable to the institution.

The institution's objectives should be established by determining priorities in the event of major incidents. These priorities could include protecting employees, ensuring the institution's financial survival, complying with the laws and regulations in force and maintaining essential services to clients.

[7] Autorité des marchés financiers, *Outsourcing Risk Guideline*.

Resources, which are generally scarce in the event of major incidents, cannot be allocated effectively without clear and precise objectives. The objectives set by the institution will allow it to design a BCP tailored to its risk profile.

5. Development and implementation of the business continuity plan

Principle 6: Business continuity planning

> The AMF expects a financial institution to develop and implement a BCP outlining the actions to be taken in the event of a major operational incident that will have an impact on its critical activities.

The BCP is the principal tangible component of a financial institution's sound business continuity management. As such, it should be clear, practical, tested and updated regularly. It should also be accompanied by a communications plan.

The financial institution should plan for the continuity and resumption of its business activities by putting into place appropriate response measures. These measures should describe in detail the means for ensuring the continuity of critical activities at a minimum level of service and within an acceptable period of time, particularly when the usual resources are not available. In this regard, when developing its BCP, the financial institution should set out the measures it intends to adopt, based on the following elements:

- organizational: development of policies, procedures, action plans, emergency measures, reliability reviews, updating, etc.;
- human: awareness campaigns, training, etc.;
- technological: software, equipment, databases, networks, etc.; and
- physical and material: infrastructures, recovery sites, etc.

The following subsections elaborate on some of these elements.

5.1 Mitigating the threat of major operational incidents

Mitigating risks is a permanent process that should be conducted even if the BCP has not been activated. For example, if an institution requires electricity to maintain its critical activities, it can mitigate the risk of a short-term power outage by installing generators.

5.2 Recovery sites

The institution should have access to one or more recovery sites in the event it can no longer use its primary sites or physical assets, networks or information technology applications. In selecting the recovery sites, the financial institution should consider several factors, including the nature of the major operational incidents that pose a threat to the institution, the acceptable duration of an interruption and the costs. The financial institution should also consider these factors in choosing sites, to ensure that they suit its business continuity objectives and risk tolerance levels.

Recovery sites should be located far enough from primary sites so that they are not subject to the same disruptions as the primary sites. They should therefore not depend on the same systems or infrastructures as the primary sites, and should function on a different power grid and telecommunications network.

5.3 Awareness campaigns and training programs

In order to instill a business continuity management culture within the institution, employees should be informed and reminded of their responsibilities within the scope of the BCP. Training should be provided

to employees with primary responsibilities in order to ensure that they have mastered and understand the guidelines set out in the BCP and that they are in a position to apply them properly.

5.4 Communication

Successful deployment of the BCP depends on coherent, clear and effective communication in order to contain rumours, for example. Sound organization of communications is essential to maintain contact with the media, emergency services, partners and suppliers, so as to reassure employees and clients.

Principle 7: Verification of the reliability of the BCP and updating thereof

> The AMF expects a financial institution to periodically verify the reliability of its BCP. The AMF also expects the business continuity management process to be a dynamic one that takes into account any changes affecting the financial institution, outside parties and its environment.

Technological and procedural changes as well as changes in the roles and responsibilities of employees may affect the BCP's reliability. It is therefore important that its reliability be verified on a regular basis. The financial institution should ensure that deploying the BCP will allow it to continue to maintain its critical activities effectively and efficiently.

Depending on the nature and complexity of critical activities and the availability of time and resources, the financial institution could carry out modular testing at various intervals and on a regular basis. Senior management and those employees who will be involved in business continuity management should participate in these exercises so as to familiarize themselves with their roles and responsibilities within the scope of the BCP. The exercises should allow the following, in particular, to be verified:

- individual BCP components;
- connectivity and functionality of tools, systems and recovery sites;
- qualitative elements (time required to resume operations) and quantitative elements (capacity for resuming operations);
- validity of planning assumptions; and
- co-ordination with business partners and government authorities.

For an overall picture of the business continuity strategy, the institution should carry out exercises that integrate core BCP components. The financial institution could also gradually increase the difficulty of its exercises by adding new scenarios, thereby enhancing BCP reliability tests.

A report should be prepared at the end of each exercise. Depending on the results obtained, the necessary solutions or remedial actions should be incorporated into the BCP and an amended version produced.