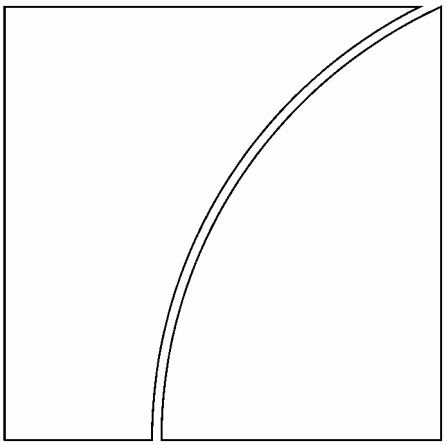
Basel Committee
on Banking Supervision

The Joint Forum



High-level principles for business continuity

August 2006

BANK FOR INTERNATIONAL SETTLEMENTS

Requests for copies of publications, or for additions/changes to the mailing list, should be sent to:

Bank for International Settlements
Press & Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org
Fax: +41 61 280 9100 and +41 61 280 8100

ISBN print: 92-9131-722-5
ISBN web: 92-9197-722-5

THE JOINT FORUM

BASEL COMMITTEE ON BANKING SUPERVISION
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS
C/O BANK FOR INTERNATIONAL SETTLEMENTS
CH-4002 BASEL, SWITZERLAND

High-level principles for business continuity

August 2006

Table of contents

Glossary

Alternate site	A site held in readiness for use during a *business continuity* event to maintain an organisation's *business continuity*. The term applies equally to work space or technology requirements. Organisations may have more than one *alternate site*. In some cases, an *alternate site* may involve facilities that are used for normal day-to-day operations but which are able to accommodate additional business functions when a primary location becomes inoperable. Examples of *alternate sites* include relocation and disaster recovery sites, whether managed directly or maintained by a third party for an organisation's exclusive use or for use by multiple organisations.
Business continuity	A state of continued, uninterrupted operation of a business.
Business continuity management	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.
Business continuity plan	A component of *business continuity management*. A *business continuity plan* is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organisation in the event of a disruption.
Business impact analysis	A component of *business continuity management*. *Business impact analysis* is the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify *recovery* priorities, *recovery* resource requirements, and essential staff and to help shape a *business continuity plan*.
Communication protocols	Established procedures for communicating that are agreed in advance between two or more parties internal or external to an organisation. Such procedures typically include the methodology for transmitting, writing, and reading of data (eg e-mails and intranet for employees, teleconferences or meetings with identified internal or external parties, and press releases, website postings, or news conferences for the public or other external stakeholders). Such procedures also typically include the nature of information that should be shared with various internal and external parties and how certain types of information should be treated (eg public or non-public),

Critical market participants	Participants in financial markets that perform *critical operations* or provide *critical services*. Their inability to perform such operations or provide such services for their own or others' benefit could pose a significant risk of major disruption to the continued operation of individual participants or the financial system.
Critical operation or service	Any activity, function, process, or service, the loss of which would be material to the continued operation of the *financial industry participant*, *financial authority*, and/or financial system concerned. Whether a particular operation or service is "critical" depends on the nature of the relevant organisation or financial system. Data centre operations are an example of *critical operations* to most *financial industry participants*. Examples of *critical services* to financial systems include, but are not limited to, large value payment processing, clearing and settlement of transactions, and supporting systems such as funding and reconciliation services.
Emergency response organisation	An organisation responsible for responding to hazards to the general population (eg fire department, police services).
Financial authorities	A financial sector regulatory or supervisory organisation having some level of responsibility for safeguarding, and maintaining public confidence in, the financial system. Examples include prudential supervisors of securities firms, insurance companies, and banks and other deposit-taking institutions, as well as financial services consumer protection agencies and authorities with responsibility for stock and commodities exchanges. Non-supervisory central banks are included in their capacity as overseers of *payment and settlement systems*.
Financial industry participants	Financial institutions and other organisations that participate in the banking, securities and/or insurance sectors and that are subject to some level of regulation or supervision by one or more *financial authorities*. Examples include banks, securities firms, insurance companies, stock exchanges, operators of *payment and settlement systems* (including central banks that provide such services), messaging service providers (such as SWIFT), and self-regulatory organisations.
International standard setting organisations	Organisations whose responsibilities include defining prudential and other standards applicable to a specific group of *financial industry participants* operating in a particular financial services sector and in a geographic region encompassing more than one country. Examples include the Basel Committee on Banking Supervision (www.bis.org/bcbs), the International Organisation of Securities Commissions (www.iosco.org), the International Association of Insurance Supervisors (www.iaisweb.org), the standard setters for the banking, securities and insurance sectors respectively, and the Committee on Payment and Settlement Systems (www.bis.org/cpss), a forum for coordinating the oversight functions of central banks with respect to payment systems.

Major operational disruption	A high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it. In addition to impeding the normal operation of *financial industry participants* and other commercial organisations, *major operational disruptions* typically affect the *physical infrastructure.* *Major operational disruptions* can result from a wide range of events, such as earthquakes, hurricanes and other weather-related events, terrorist attacks and other intentional or accidental acts that cause widespread damage to the *physical infrastructure*. Other events, such as technology viruses, pandemics and other biological incidents, may not cause widespread damage to the *physical infrastructure* but can nonetheless lead to *major operational disruptions* by affecting the normal operation of the *physical infrastructure* in other ways. Events whose impact is most significant are referred to as "extreme events". They involve one or more of the following: the destruction of, or severe damage to, *physical infrastructure* and facilities; the loss or inaccessibility of personnel; and, restricted access to the affected area.
Operational risk	The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
Payment and settlement system	A system consisting of a group of member firms and a set of instruments and procedures for the transmission and settlement of payments or financial instruments between members.
Payment and settlement system operator	An organisation that provides the processing services for transactions sent by participants in the *payment and settlement system*. The services provided could include the generation or processing of operational data, effecting of controls and security measures, and the clearing and settlement of payments or other obligations.
Physical infrastructure	Those assets, facilities and services provided by non-*financial industry participants* and widely depended on by business, governments and individuals for day-to-day activities. Examples include water, public health, emergency services, telecommunication and information services, energy, and transportation.
Recovery	The rebuilding of specific business operations following a disruption to a level sufficient to meet outstanding business obligations.
Recovery level	An element of a *recovery objective. Recovery level* is the target level of service that will be provided in respect of a specific business operation after a disruption.

Recovery objective	A pre-defined goal for recovering specified business operations and supporting systems to a specified level of service (*recovery level*) within a defined period following a disruption (*recovery time*).
Recovery time	An element of a *recovery objective. Recovery time* is the target duration of time to recover a specific business operation. A r*ecovery time* has two components: the duration of time from the disruption to the activation of a *business continuity plan*; and, the duration of time from the activation of the *business continuity plan* to the *recovery* of the specific business operation.
Resilience	The ability of a *financial industry participant, financial authority* or financial system to absorb the impact of a *major operational disruption* and continue to maintain *critical operations or services*.

High-level principles for business continuity

Background and context

1. *Business continuity* is an ongoing priority for *financial industry participants* and *financial authorities*.[1] Recent acts of terrorism in New York, London, Istanbul, Madrid and elsewhere, outbreaks of Severe Acute Respiratory Syndrome (SARS) and the Avian Flu, and various widespread natural disasters have served to heighten that priority by underlining the substantial risk of *major operational disruptions* to the financial system.

2. *Financial authorities* and *financial industry participants* have a shared interest in promoting the *resilience* of the financial system to *major operational disruptions*. This interest is the result of multiple factors, including:

- The pivotal role that financial intermediation plays in facilitating and promoting national and global economic activity by providing the means for making and receiving payments, for borrowing and lending, for effecting transactions, for insuring risks, and for raising capital and promoting investment;
- The concentration of clearing and settlement processes in most financial systems. Disruptions of these processes can have material adverse consequences for a financial system and prevent significant market participants from completing transactions and meeting their obligations;
- Deepening interdependencies among *financial industry participants* within and across jurisdictions. The velocity with which money and securities turn over on a daily basis underpins the considerable interdependencies – in the form of settlement risk and, ultimately, credit and liquidity risks – among *financial industry participants* and investors. The result is that operational disruptions at one *financial industry participant* can cause difficulties at others. Furthermore, given the increasing globalisation of markets, disruptions in one jurisdiction could have serious implications for others through contagion effects;
- The possibility of terrorist or other malicious attacks targeted, directly or indirectly, at the infrastructure of the financial system;
- The importance of public confidence in the ability of financial systems to function smoothly. Repeated or prolonged interruptions to the operation of a financial system undermine confidence and could result in a withdrawal of capital from that system by domestic and global participants.

3. At the same time, however, other factors such as the increasing complexity and *operational risk* in all areas of the financial system add to the challenge of promoting its *resilience*. For example, the financial system is keenly dependent on automation and, in turn, on those elements of the *physical infrastructure* that support automation, such as telecommunications and power. While the organisations that provide the facilities and services comprising the *physical infrastructure* are actively engaged in efforts of their own to improve their resilience to *major operational disruptions*, *financial authorities* and *financial*

[1] "Business continuity", "financial industry participants", "financial authorities" and other key terms are defined for purposes of this paper in the Glossary. For ease of identification, all terms defined in the Glossary are italicised when they are used in the paper.

industry participants have no direct control over their decisions when *major operational disruptions* occur.

4. *Financial authorities* in some of the key financial centres have been working closely with *financial industry participants* to establish a consensus as to what constitutes acceptable standards for *business continuity*. This effort has been supported by recent private sector initiatives. For example, a number of groups have been established for the purpose of coordinating *financial industry participants'* work in the area of *business continuity management.*[2,3] In addition, some financial sector trade associations have taken a leading role in promoting sound *business continuity management* among their memberships through, for example, the publication of guidance on sound practices.[4] Much of this work to date has been focussed at the national level. As a result, while the work has shared the same broad objective (ie enhancing the *resilience* of the financial system), it has generated a variety of outcomes, including the development of requirements and guidance by *financial authorities* in some jurisdictions.

5. Consistent with their focus on preserving the functionality of a financial system as a whole, *financial authorities* undertaking these initiatives have tended to give priority to *critical market participants*. The lessons learned from past experience, however, are applicable to a broader audience.

6. At the international level, while there have been several regulatory initiatives on the *business continuity* front, they have been concentrated mainly on coordinating cross-border communications in a crisis. For example, EU members signed an updated Memorandum of Understanding in May 2005 on information exchange during a financial crisis; all of the signatories are EU regulators, central banks and finance ministries. Examples of international *business continuity* initiatives with a broader focus include meetings of the Committee on Payment and Settlement Systems where central bank participants share their experiences in reviewing and enhancing *business continuity plans*. The Joint Task Force on Crisis Management, created by the Committee of European Banking Supervisors and the Banking Supervision Committee of the European Central Bank to formulate guidance and identify best practices for crisis management, is an example of similar initiatives at a regional level. To date, however, there has not been a concerted effort to draw together the lessons learned from major events and translate them into a set of *business continuity* principles that is relevant across national boundaries and financial sectors (ie banking, securities, and insurance).

7. In the summer of 2004, the Financial Stability Forum and the Bank of England co-hosted a symposium on *business continuity* issues. Based on the findings of the symposium, the Financial Stability Forum asked the sectoral standard setting bodies (the Basel Committee on Banking Supervision (BCBS), the International Organisation of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS)) or the Joint Forum to review approaches to *business continuity* across countries and financial

---

[2] Conceptually, *business continuity management* is distinct from financial crisis management in that a financial crisis does not typically entail *business continuity* concerns. An event that gives rise to *business continuity* concerns, however, could develop into a financial crisis.

[3] Examples of private sector groups include the Securities Industry Business Continuity Management Group, an informal industry forum of the Securities Industry Association (www.sia.com), and ChicagoFIRST, a non-profit association dedicated to addressing emergency management issues affecting financial institutions and requiring a coordinated response (www.chicagofirst.org), in the United States.

[4] One example is "A Guide to Business Continuity Management" published in January 2003 by the British Bankers' Association (www.bba.org.uk).

sectors and consider whether it might be appropriate to develop high-level principles that could apply across the financial system globally.

8. The Joint Forum's parent organisations (BCBS, IOSCO and IAIS) confirmed in November 2004 that the Joint Forum should undertake such a review. Following an initial scoping exercise, the Joint Forum concluded in February 2005 that high-level principles on *business continuity* would contribute beneficially to the *resilience* of the global financial system. A formal working group of the Joint Forum (see Annex VII for a list of working group members) developed a set of high-level principles that were published in a consultative paper in December 2005. This paper is a revised version of the December 2005 consultation draft.

Effective business continuity management

9. *Business continuity management*, a significant component of *operational risk* 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. Effective *business continuity management* concentrates on the impact, as opposed to the source, of the disruption, which affords *financial industry participants* and *financial authorities* greater flexibility to address a broad range of disruptions. At the same time, however, organisations cannot ignore the nature of the risks to which they are exposed. For example, organisations located in earthquake-prone regions commonly plan for the impact of earthquake-related *major operational disruptions*.

10. Effective *business continuity management* typically incorporates *business impact analyses, recovery* strategies and *business continuity plans* as well as testing programmes, training and awareness programmes, and communication and crisis management programmes.

- A *business impact analysis* is the starting point – it is a dynamic process for identifying *critical operations and services*, key internal and external dependencies and appropriate *resilience* levels. It assesses the risks and potential impact of various disruption scenarios on an organisation's operations and reputation.
- A *recovery* strategy sets out *recovery objectives* and priorities that are based on the *business impact analysis*. Among other things, it establishes targets for the level of service the organisation would seek to deliver in the event of a disruption and the framework for ultimately resuming business operations.[5]
- *Business continuity plans* provide detailed guidance for implementing the *recovery* strategy. They establish the roles and allocate responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that disables key personnel. They also clearly set out the decision-making authority and define the triggers for invoking the

[5] The ultimate objective of a *business continuity plan* is the full restoration of an organisation's operations to the point where the organisation is able to resume normal business operations. Most plans sequence the *recovery* of operations according to their business impact, focussing first on an organisation's *critical operations*.

organisation's *business continuity plan*. The safety of staff should be the paramount consideration of an organisation's *business continuity plan*.

The benefits of high-level principles

11. The high-level principles set out in this paper are intended to support *international standard setting organisations* and national *financial authorities* in their efforts to improve the *resilience* of financial systems to *major operational disruptions*. They are not sufficiently detailed to substitute for sectoral or national arrangements and are not intended for this purpose. Rather, they provide a broad framework for *international standard setting organisations* and national *financial authorities* to use in developing *business continuity* arrangements that are more detailed and more closely tailored to their unique sectoral and local circumstances. They also provide a consistent context for those arrangements and, in so doing, promote a common base level of *resilience* across national boundaries. Moreover, given the global nature of the financial industry and the role of *financial authorities* as the focal point for cross-border information exchange and action in the event of a *major operational disruption*, the principles encourage enhancements to the cross-border communication channels that would be used during such disruptions.

12. The high-level principles set out in this paper are therefore not intended to be prescriptive, nor are they directed exclusively at those *financial industry participants* considered to be *critical market participants*. Rather, they constitute a broad framework of sound practice relevant to all *financial industry participants* and *financial authorities* in all jurisdictions. Broad applicability of the high-level principles, however, does not mean a one-size-fits-all approach to *business continuity*. An organisation's *business continuity management* should be proportionate to its business risk (arising from both internal and external sources) and tailored to the scale and scope of its operations.

13. Operational disruptions of varying kinds and impact are commonplace – organisations routinely accommodate such risks as computer malfunctions, power failures and transportation disruptions in their *business continuity plans*. From a corporate perspective, *resilience* to operational disruptions has a clear commercial rationale – customers of organisations whose systems are prone to regular failure as a result of relatively common events will inevitably choose to do business with more resilient competitors. In a competitive environment, an organisation typically will weigh its direct benefit from measures to improve its *resilience* to operational disruptions against the cost of those measures.

14. Similar cost-benefit considerations apply to measures for improving a financial system's *resilience* to operational disruptions. The benefits of improved systemic *resilience* accrue to all participants in that system (albeit to a varying extent), but in most cases such improvements are the result of investments in *business continuity* by individual *financial industry participants*. Because *financial industry participants* typically consider only their direct benefits and costs whereas *financial authorities* are expected to consider the broader public interest dimension, a natural tension exists between the levels of *resilience* that *financial industry participants* might consider reasonable for their own business purposes and the objectives of *financial authorities* for the *resilience* of the financial system as a whole. Recognising the shared interest in improving the *resilience* of the financial system, the high-level *business continuity* principles set out in this paper represent an attempt to delineate a measured approach to *business continuity* that is sufficient in terms of its impact on the overall *resilience* of a financial system and, at the same time, proportionate to the risks posed by particular *financial industry participants*. Without diminishing the authority of *financial authorities* to ultimately determine the appropriate level of systemic *resilience*, an

ongoing dialogue between all affected parties, reinforced through appropriate joint exercises and testing, should produce a reasonable and responsible outcome.

15. In formulating the high-level principles, careful account has been taken of the lessons learned from recent instances of *major operational disruption*, some of which are summarised in the case studies set out in Annexes I to V. These case studies illustrate the general applicability of the principles. In addition, for each lesson learned a specific reference to the relevant principle is provided. Care was also taken to avoid unnecessary duplication of work that has already been undertaken in the *business continuity* area. A bibliography of the publications considered in the development of the principles is provided in Annex VI.

Target audiences

16. The high-level *business continuity* principles in this paper have been developed for two distinct but related audiences – *financial industry participants* and *financial authorities*. While these groups have different perspectives, roles and responsibilities in the event of a *major operational disruption*, both are integral in any meaningful effort to improve the financial system's *resilience* to such disruptions. The same effort will not be required of every organisation in these groups to achieve the objectives of every principle in this paper. In fact, many organisations in both groups already have effective and comprehensive approaches to *business continuity management*. There are organisations in both groups, however, whose careful attention to these principles would not only improve their *resilience* to *major operational disruptions* but yield benefits for the *resilience* of the financial system more broadly.

Financial industry participants

17. For the purpose of this paper, the term *financial industry participants* should be understood in its broadest sense so that it captures not only financial institutions such as banks, securities firms, and insurance companies, but also those organisations that provide services that are necessary for financial systems to operate, such as stock and commodities exchanges, self-regulatory organisations, and *payment and settlement system operators*.[6]

18. Within this broad target audience, there is a subset of participants that provide *critical services* to financial systems. Large value payment processing and securities settlement are examples of *critical services* in a financial system. A disruption of the services provided by these participants, for which there are no viable immediate substitutes in many cases, would have a cascading effect on the financial system. In addition, in some markets there may be *financial industry participants* whose inability to continue normal operations could, because of the significance of their role in those markets, affect other participants in those markets and thereby have a cascading effect on the financial system. For these *financial industry participants*, there is an inevitable step-up in their obligation to ensure a high degree of *resilience* in the event of a *major operational disruption*. In contrast, the inability of an individual *financial industry participant* to continue operating in the event of a

[6] Financial sector trade associations are not included in the definition of *financial industry participants*; therefore, the high-level principles in this paper do not apply to them. It is recognised nonetheless that these organisations play an important role in promoting effective *business continuity management* practices among their member firms. Depending on their roles in their respective markets, industry associations can also be helpful in other ways, such as in the planning and conducting of industry-wide tests and the development and maintenance of communication protocols.

major operational disruption generally would not render the markets in which they operate dysfunctional, except where that participant is a *critical market participant*. Principle 3 provides additional clarity on this distinction within this target audience and its implications for *business continuity management*.

Financial authorities

19. The term *financial authorities* should be understood, for the purpose of this paper, to include those organisations with financial sector regulatory or supervisory responsibilities. For example, prudential supervisory authorities with responsibilities for banks and other deposit-taking institutions, insurance companies, and securities firms are included, as are financial services consumer protection agencies and authorities responsible for overseeing financial markets. Non-supervisory central banks are also included in their capacity as overseers of *payment and settlement systems*.[7] Because the mandates of *financial authorities* vary, however, the approach to *business continuity management* that is most appropriate for one *financial authority* may not be as appropriate for another.

20. As well as having to attend to their own *business continuity* in the event of a *major operational disruption*, *financial authorities* have broader public responsibilities for safeguarding and maintaining public confidence in the financial system. For example, national governments might seek the advice of *financial authorities* regarding the deployment of resources and restoration of services. *Financial authorities* might also need to consider various types of regulatory forbearance to enable *financial industry participants* to focus on recovering *critical operations* and providing essential services to their clients. Therefore, the principles that apply to *financial authorities* explicitly incorporate the need to understand how a *major operational disruption* might affect the functioning of *financial industry participants* and the financial system as a whole, and to identify *financial industry participants* whose inability to recover their operations and resume normal business activities in a reasonable timeframe would have wider implications for the financial system. Because the mandates of *financial authorities* vary, however (eg some prudential supervisors are responsible for systemic issues while others are not), the extent to which a particular principle applies to a given *financial authority* might also vary.

[7] In light of their responsibility for broader financial stability in many jurisdictions, central banks are likely to perform various other roles in the event of a *major operational disruption*. For purposes of this paper, however, central banks' lender of last resort and monetary policy functions are not intended to be captured in this definition of *financial authorities*.

High-level principles for business continuity

21. The high-level principles that follow are applicable to both *financial industry participants* and *financial authorities* except for Principle 7, which is relevant only for *financial authorities*. Because of the different perspectives, roles and responsibilities of these two groups of organisations in the event of a *major operational disruption*, however, the way in which a particular principle applies may be different. The key differences in application are highlighted in the discussion that follows each principle.

22. The principles in this paper build upon traditional concepts of effective *business continuity management* in the following ways:

- Principle 1 emphasises that the requirement for sound *business continuity management* applies to all *financial authorities* and *financial industry participants* and that the ultimate responsibility for *business continuity management* – not unlike the management of other risks – rests with an organisation's board of directors and senior management. [8,9]
- Principle 2 advises organisations that they should explicitly consider and plan for *major operational disruptions*. While this concept may be new for many organisations, it is considered important in light of the increasing frequency of such events.
- Principle 3 states that *financial industry participants* should develop *recovery objectives* that reflect the risk they represent to the operation of the financial system. *Financial industry participants* that provide *critical services* to, or otherwise present significant risk to the operation of, the financial system should target higher standards in their *business continuity management* than other participants. This concept may be new for some *financial industry participants.* Because the steps necessary to improve the *resilience* of the financial system may be more costly than the steps such participants would choose to undertake on their own, *financial authorities* are encouraged to participate, as appropriate, in identifying *recovery objectives* that are proportionate to the risk posed by a given participant in order to achieve a reasonably consistent level of *resilience*.
- Principle 4 stresses the critical importance of *business continuity plans* addressing the full range of internal and external communication issues an organisation may encounter in the event of a *major operational disruption*. The principle specifically recognises that clear, regular communication during a *major operational disruption* is necessary to manage a crisis and maintain public confidence.
- Principle 5 highlights the special case of cross-border communications during a *major operational disruption*. Given the deepening interdependencies of financial systems across national boundaries, this principle advises *financial industry*

---

[8] This paper refers to a management structure comprising a board of directors and senior management. It is recognised, however, that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within an organisation.

[9] Not all *financial authorities* have boards, in which case references to the board or the board and senior management should be read to mean senior management.

participants and *financial authorities* to adopt *communication protocols* that address situations where cross border communication may be necessary.

- Principle 6 emphasises the need to ensure that *business continuity plans* are effective and to identify necessary modifications through periodic testing.
- Finally, to ensure that *financial industry participants* are in fact implementing appropriate approaches to *business continuity management* that reflect the *recovery objectives* adopted in accordance with Principles 1 and 3, Principle 7 calls upon *financial authorities* to incorporate *business continuity management* reviews into their frameworks for assessing *financial industry participants*.

Principle 1: Board and senior management responsibility

Financial industry participants and financial authorities should have effective and comprehensive approaches to business continuity management. An organisation's board of directors and senior management are collectively responsible for the organisation's business continuity.

23. *Business continuity management* should be an integral part of the overall risk management programme of *financial industry participants* and *financial authorities*. *Business continuity management* policies, standards and processes should be implemented on an enterprise-wide basis or, at a minimum, embedded in an organisation's *critical operations*. Comprehensive *business continuity management* addresses not only technical considerations but also the human dimension. In so doing, it recognises that employees and possibly their families may be affected by the same event that gives rise to *business continuity* concerns and that, as a result, not all employees will be available to the organisation during or immediately following the event.

24. An organisation'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. They should recognise that outsourcing a business operation does not transfer the associated *business continuity management* responsibilities to the service provider. 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*.

25. 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. An organisation'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.

26. 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 an organisation'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 organisation's response, commensurate with the severity of the disruption.

27. In the case of *financial authorities*, the board and senior management should be confident in the authority's ability to fulfil its mandate during an operational disruption that affects its own operations or those of the financial system. Accordingly, they should be satisfied that the authority's powers provide for sufficient flexibility to respond appropriately and expeditiously to the wide range of issues that might arise under such circumstances. Given the interdependencies within financial systems, it would be useful for *financial authorities* that share oversight responsibilities for a given financial system to agree on an appropriate framework for coordinating the response to *major operational disruptions* affecting that system.

Principle 2: Major operational disruptions

Financial industry participants and financial authorities should incorporate the risk of a major operational disruption into their approaches to business continuity management. Financial authorities' business continuity management also should address how they will respond to a major operational disruption that affects the operation of the financial industry participants or financial system for which they are responsible.

28. *Major operational disruptions* pose a substantial risk to the continued operation of *financial industry participants* and *financial authorities,* as well as to the operation of the financial system. Accordingly, all *financial industry participants* and *financial authorities* should incorporate the risk of a *major operational disruption* in their *business continuity plans.* The extent to which a *financial industry participant* prepares to recover from a *major operational disruption* should be based on its unique characteristics and risk profile. Because access to the resources needed for the full *recovery* of its operations may be limited during a *major operational disruption*, a *financial industry participant* should identify through a *business impact analysis* those business functions and operations that are to be recovered on a priority basis and establish appropriate *recovery objectives* for those operations.

29. During a *major operational disruption*, the operation of the financial system will be of keen importance nationally and, possibly, globally. A *financial authority* will be expected to play a major role in monitoring the status of the financial markets and *financial industry participants* for which it is responsible. Depending on its mandate, a *financial authority* might also be expected to coordinate efforts to recover *critical services* to the financial system.

30. *Major operational disruptions* vary in intensity, scope and duration. In many cases, organisations may be able to remain at their primary business locations if they have sufficient backup for power and other essential services. Recent experience, however, has demonstrated that some *major operational disruptions* constitute extreme events whose impact can be very broad in scope, duration or both. In evaluating whether their own *business continuity management* is sufficient to accommodate such *major operational disruptions*, *financial industry participants* and *financial authorities* should review the adequacy of their *recovery* arrangements in the following three important areas.

- First, an organisation should take care that its *alternate site* is sufficiently remote from its primary business location and, where possible, does not depend on the same *physical infrastructure* components. This minimises the risk that both could be affected by the same event. For example, the *alternate site* should ideally be on a different power grid and central telecommunication circuit from the primary business location.
- Second, an organisation 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.

- Third, given that staff at the primary business location are likely to be unavailable, the *business continuity plan* should address how the organisation 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, for example: specific plans to source staff from multiple geographic locations; locating staff at *alternate sites* on a permanent basis (eg in the case of load-sharing); 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; and hiring employees who live at the outer edges of typical commuting ranges from the primary business location.

Principle 3: Recovery objectives

Financial industry participants should develop recovery objectives that reflect the risk they represent to the operation of the financial system. As appropriate, such recovery objectives may be established in consultation with, or by, the relevant financial authorities.

31. A *financial industry participant* that experiences a *major operational disruption* might affect the ability of other *financial industry participants* – and possibly the financial system – to continue normal business operations. Accordingly, *financial industry participants* 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 financial system. Relevant *financial authorities* are encouraged to provide guidance that would assist *financial industry participants* in making this assessment. Examples include a *payment and settlement system operator* on which *financial industry participants* depend to process and complete transactions – particularly where there are no others capable of substituting for that operator – or *financial industry participants* that play a significant role in providing financial services within a particular region.

32. *Financial industry participants* should establish *recovery objectives* that are proportionate to the risk they pose to the operation of the financial system. The board and senior management are ultimately accountable for the organisation's *recovery objectives*, although in practice *recovery objectives* that apply to individual business lines are often developed by, or in consultation with, business line management. *Financial authorities* are encouraged to participate in the identification of *recovery objectives* where such a role is consistent with an authority's mandate. The highest *recovery objectives* typically should be reserved for those *financial industry participants* that are most likely to disrupt the 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 within-the-day-of-disruption *recovery time objective* in the case of *major operational disruptions* resulting from discrete events,[10] and generally be expected not only to recover *critical operations and services* but also to resume normal business in those areas within the same timeframe. It may be acceptable for other participants to target a less stringent *recovery time* depending on the

[10] The concept of within-the-day-of-disruption recovery may not be as applicable in the case of events such as a pandemic whose duration may stretch to weeks as opposed to a day or less. Even in those cases, however, the general expectation that certain *financial industry participants* would target higher *recovery objectives* would continue to be relevant.

impact a disruption of their operations would have on the financial system or on the expectations of other *financial industry participants.* In assessing the reasonableness of an organisation's *recovery objectives*, *financial authorities* are strongly encouraged to consider the increased risk of failed transactions, liquidity dislocations, solvency problems, and loss of confidence that accompany prolonged disruptions in the financial system.

33. *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 *financial industry participants* with benchmarks for testing the effectiveness of their *business continuity management*. They also provide some assurance that *financial industry 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.

Principle 4: Communications

Financial industry participants and financial authorities should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties in the event of a major operational disruption.

34. The ability to communicate effectively with relevant internal and external parties in the event of a *major operational disruption* is essential for *financial industry participants* and *financial authorities* alike. Particularly in the early stages of a disruption, effective communication is necessary to gauge the impact of the disruption – on an organisation's staff and operations, and on the broader financial system – and make appropriate decisions about whether to invoke a *business continuity plan*. 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 *financial industry participant* or in the financial system as a whole, requires clear, regular communication throughout the duration of a *major operational disruption*.

35. Accordingly, and also because of the added pressure that is often associated with decision-making during a *major operational disruption*, the *business continuity plans* of *financial industry participants* and *financial authorities* should incorporate comprehensive emergency *communication protocols* and procedures. For example, a *financial industry participant* would need to consider the external parties with whom it should communicate, such as the relevant *financial authorities*, other *financial industry participants*, the public and other stakeholders, as well as how best to communicate with them and within its own organisation. It may also be necessary for a participant to obtain information from *financial authorities* and other *financial industry participants* regarding the status of the financial system, as well as from organisations that provide *physical infrastructure* services regarding the status of any services required for the implementation of the participant's *business continuity plan*. A *financial authority* will need to consider similar issues, but its emergency communication procedures should also reflect its broader responsibilities. For example, a *financial authority* may want to consider issuing public statements during a crisis to assure the markets and the public that appropriate measures are being taken and inform them of those measures. In cases where *financial authorities* share oversight responsibilities for a group comprising more than one *financial industry participant*, it may be beneficial for those

authorities to designate one from their midst as the "coordinator" for purposes of facilitating communication during a *major operational disruption* affecting the group.[11]

36. The communication procedures of *financial industry participants* and *financial authorities* generally should:

- 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;
- Build on any *communication protocols* that already exist within the financial system and include contact information for relevant domestic *financial authorities* and *financial industry participants* to facilitate an assessment of the condition of the financial system and coordinate *recovery* efforts. Examples of existing *communication protocols* might include conference call schedules developed by financial sector trade associations or *financial authority* working groups and bilateral communication procedures between major international exchanges. In addition, consideration should be given to including contact information for officials with local *emergency response organisations* where critical facilities are located;
- 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 (eg digital and analogue land line phones, mobile phones, satellite phones, text messaging, websites, hand-held wireless devices, etc);
- In the case of *financial authorities*, include, as appropriate, contact information for national or regional protection and intelligence agencies and other relevant governmental authorities. These arrangements may require the use of secure communications using specialised "secure" telephones, faxes, and emails; and,
- Provide for the regular updating of calling trees and other contact information and the periodic testing of calling trees.

Principle 5: Cross-border communications

Financial industry participants' and financial authorities' communication procedures should address communications with financial authorities in other jurisdictions in the event of major operational disruptions with cross-border implications.

37. Because of the deepening interdependencies among *financial industry participants* across jurisdictions, it is increasingly likely that the impact of a *major operational disruption* will extend across national borders. Addressing disruptions that cross national borders introduces additional complexity. Although domestic communication procedures may be reasonably well-defined in the *business continuity plans* of many *financial industry participants* and *financial authorities*, special attention is warranted in preparing for disruptions with international scope.

---

[11] For a more in-depth discussion of the "coordinator" concept, see *Coordinator Paper*, Joint Forum, February 1999 (http://www.bis.org/publ/joint02.pdf#page=105).

38. *Financial industry participants* should consider the possibility that a disruption of their business operations in one jurisdiction would affect significant subsidiary or branch operations or otherwise affect the financial system in other jurisdictions. Where this outcome is possible, a *financial industry participant's communication protocols* should address the circumstances under which it would contact the relevant non-domestic *financial authorities*. *Financial authorities* should incorporate *communication protocols* in their *business continuity plans* for communicating with *financial authorities* in other jurisdictions in the event of a *major operational disruption* that affects (or could affect) the continued operation of the international financial system. Although it was developed to address financial crises and not *business continuity* events, per se, the *Memorandum of Understanding on co-operation between the Banking Supervisors, Central Banks and Finance Ministries of the European Union in Financial Crisis situations (2005)*[12] provides a useful example of what such *communication protocols* might entail. It comprises a set of principles and procedures for sharing information, views and assessments among the authorities potentially involved in a crisis situation, as well as arrangements for the development of contingency plans for the management of crisis situations and stress testing and simulation exercises.

39. These *communication protocols* should build on existing cross-border relationships and multi-jurisdictional protocols by identifying the types of officials at *financial authorities* who might need to be involved in responding to such disruptions and including the relevant contact information. Examples of existing contact lists include the Crisis Management Contact List maintained by the Financial Stability Forum covering central banks, supervisory agencies, finance and treasury departments, and key international financial institutions in some 30 countries and the Bank Supervisors' Contact List maintained by the BCBS listing supervisory contacts around the world.[13] It is likely that communication with *financial authorities* in other jurisdictions would take place at several levels simultaneously, with senior decision-makers and more technical or specialised staff members in one organisation holding discussions with their respective counterparts at the other.

40. *Financial authorities*, in particular, are encouraged to hold periodic discussions with relevant *financial authorities* in other jurisdictions to develop a shared understanding of the events that could have significant cross-border effects on the financial system and agree on procedures for communicating with one another under such circumstances and the issues that should be addressed. The issues that might be covered in the event of cross-border disruptions would include, for example, the impacts of the disruption in their respective markets and its contagion effects, if any; issues involving emergency closures or suspensions of major markets; changes in trading hours or clearing and settlement periods; and, the details of any regulatory forbearance that may have been extended.

Principle 6: Testing

Financial industry participants and financial authorities should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate.

41. Testing the ability to recover *critical operations* as intended is an essential component of effective *business continuity management*. Such testing, which can take many forms, should be conducted periodically, with the nature, scope and frequency determined by

---

[12] The MOU is a confidential document and is not available to the general public. The press release that accompanied the MOU's publication in May 2005 includes information about its objectives, contents and signatories.

[13] These contact lists are prepared for their respective constituencies and are not available to the general public.

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 some cases, this need could arise as a result of 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. Senior management and the board should ensure that any gaps or shortcomings reported to them are addressed in an appropriate and timely manner.

42. *Financial authorities* should strongly encourage *financial industry participants* that present risk to the financial system to conduct tests from their *alternate sites* with relevant *critical market participants* and *payment and settlement system operators*. *Financial authorities* and key *financial industry participants* are also encouraged to participate in market- or industry-wide tests to assess the level of *resilience* across markets and the compatibility of the *recovery* strategies of individual participants. In light of the substantial costs involved, the decision to undertake a market- or industry-wide test should be based on a thorough cost-benefit analysis.

43. In addition to ensuring that *business continuity plans* are evaluated and updated as necessary, 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.*

Principle 7: Business continuity management reviews by financial authorities

Financial authorities should incorporate business continuity management reviews into their frameworks for the ongoing assessment of the financial industry participants for which they are responsible.

44. *Financial authorities* should expect *financial industry participants* to develop and implement effective *business continuity management* that is updated on an ongoing basis. *Financial authorities* should incorporate *business continuity management* reviews into their frameworks for the assessment of *financial industry participants*. The nature, scope and frequency of the reviews will be determined by the requirements of their regulatory or supervisory frameworks. Assessments should give due consideration to whether a participant's *business continuity management,* including its *recovery objectives*, is appropriate for the size and scope of its business and the risk the participant presents to the continued operation of the financial system. *Financial authorities* should also assess whether participants are taking appropriate steps to augment their *business continuity management*, where necessary. Where *financial authorities* share responsibility for the same *financial industry participant*, it would be useful for those authorities to agree on a framework for coordinating those reviews.

45. In the course of reviewing a participant's *business continuity management*, a *financial authority* should assess whether the testing programme provides adequate assurance that business processes can be recovered as intended.

Annex I

Case Study: US-Canadian electrical power grid outages in August 2003

Event

1. On Thursday 14 August 2003, cascading failures of electrical power grids in the northeast United States and most of eastern Ontario, Canada resulted in power outages that, in some areas, lasted well into the weekend.

Impact

2. Without warning, the grid failures shut down utility electrical power in financial centres such as New York City and Toronto starting around 16:11 local time on 14 August. Backup electrical power systems at securities exchanges, clearing organisations, and a large number of *financial industry participants* in the affected areas were activated automatically, enabling those organisations to avoid a sudden disruption in their systems or loss of essential data. Because the outage occurred near the normal end of the business day and perhaps because of initial uncertainties over whether the outage was the result of a terrorist attack, people were sent home by their employers or otherwise chose to evacuate the New York financial district – many left on foot because street traffic was jammed and mass transit was largely inoperable. No panic was evident, however, perhaps as a result of public statements by local and federal officials within an hour of the start of the event that there was no evidence that the power outage was terrorist-related. The financial system and its participants were largely able to complete their end-of-day operations in an orderly fashion.

3. The electrical outage continued in New York City and Toronto overnight and into the next day (15 August). Most major US and Canadian equity markets were able to maintain normal trading hours that day, while bond markets held an abbreviated trading session to allow traders more time to head home for the weekend. Wholesale and retail payments and trading and settlements proceeded with only a few delays. The large majority of banks had established backup power at larger branches and retail banking services were adequate to meet consumer needs, although numerous stand-alone ATMs stopped functioning on Thursday night. Individual bank branches that did not have backup power were closed on Friday. In a few cases, all of a US rural bank's operations were closed for all of Friday due to lack of power.

4. The sector experienced some telecommunication problems related to the power outage. Some of these problems affected entire telecommunication networks that had insufficient backup power at some central office switches. In other cases, some firms found that their backup electrical generators did not support their internal telephone systems, rendering their digital telephones inoperable, while their analogue-line telephones (which receive power over their land lines and bypass internal telecommunication switching systems) continued to function. In addition, mobile phones soon became inoperable due to message congestion, insufficient backup power at transmission and relay sites, and the inability of individuals to recharge their mobile phones' batteries.

5. There were no discernable effects on consumer confidence in the US or Canadian financial systems. On the whole, consumers were patient and proved able to cope with the situation, including the temporary loss of access to local branches and ATM machines. There were no unusual currency demands or runs on banks, nor were there any sell-offs in mutual fund markets.

Response

6. A number of *financial industry participants*, particularly organisations that support *payment and settlement systems,* responded to the outage by activating their backup power generators. Many also activated their *alternate sites* as a precautionary measure.

7. Many other organisations had provided for abundant backup power at their primary sites as part of their *business continuity plans* and did not need to relocate because there was no immediate threat to the safety of their personnel. Given the disruption of mass transit, many of these organisations implemented plans to have key staff remain overnight at or near their primary sites to ensure that *critical operations* could be maintained.

8. Some *financial industry participants* that chose not to activate their *alternate sites* were subsequently confronted with unanticipated problems. For example, the American Stock Exchange (Amex) did not activate its remote alternative trading floor because the exchange's primary trading floor appeared to have sufficient backup electrical power. At around 2:00 on 15 August, however, utility-provided steam power to the air conditioning systems that are essential for maintaining the exchange's electronic systems began to fail at Amex's primary trading floor. By the time the problem was discovered, there was insufficient time to activate and staff the *alternate site* (which was unaffected by the steam power failure in Manhattan). Instead, Amex held an abbreviated trading session on 15 August after a backup generator was located and installed.

9. US and Canadian *financial authorities* activated *communication protocols* with their respective *critical market participants* and other domestic *financial authorities*. *Financial authorities* conducted a series of calls with their affected institutions in the evening of 14 August and throughout 15 August to determine how they were coping with the outage and whether they required assistance in maintaining *critical operations*. In addition, *financial authorities* held a series of inter-agency conference calls throughout the event that provided an opportunity for banking, securities, and futures regulators to share information on how each sector was responding to the emergency.[14]

10. US *financial authorities* invited officials from the New York City Office of Emergency Management (NYCOEM) to participate in conference calls with the exchanges and clearing organisations about how this major financial centre was responding to the infrastructure failure. In these calls, NYCOEM officials were able to provide vital information concerning the status of local power, telecommunication, and transportation services and probable

[14] Many large international exchanges have reciprocal *communication protocols* that are designed to share critical information concerning developments at one exchange that might affect trading in products that are traded on other exchanges. For example, following the events of 11 September 2001, officials at leading US exchanges kept their counterparts at exchanges in Asia, Europe, and North and South America informed about when US trading was likely to resume. This was not an issue during the 2003 power outage, however, because the NYSE and NASDAQ both issued news releases around 18:00 on 14 August indicating that they planned to trade normally the next day, thereby avoiding the need to call officials at other international exchanges.

restoration schedules. In addition, when NYCOEM officials learned of Amex's problems with utility-supplied steam power, NYCOEM officials were able to assist the exchange by arranging for the installation of a backup steam generation boiler, which enabled Amex to conduct an abbreviated trading session on 15 August.

11. Announcements made by national security officials and local government officials shortly after the commencement of the outage may have contributed to consumer confidence. Moreover, consumer confidence appears to have been strengthened by the fact that the financial services sector, including highly visible organisations such as the stock exchanges, remained largely operational.

Lessons learned

12. Upon restoration of the power supply, *financial authorities* in the United States and Canada analysed how they and their *financial industry participants* responded to the challenges posed by this *major operational disruption*. Overall, these "lessons learned" exercises indicated that:

- *Business continuity plans* and *resilience* appropriate to the risk that particular *financial industry participants* pose to the financial system are paramount in maintaining *critical operations* in the face of *major operational disruptions* such as those arising from a massive infrastructure failure. (*Principles 1, 2 and 3*)
- *Business continuity plans* benefit from incorporating a broad view of the potential impacts of a *major operational disruption*, including the loss of components of the *physical infrastructure* that may not have been experienced previously. Thorough testing of procedures and systems is useful in identifying and addressing otherwise unanticipated problems with *critical operations* during a *major operational disruption* (eg the failure at some firms to have sufficient backup power to support their telecommunication systems and Amex's assumption that its steam power supplies would not be interrupted in an electrical power outage). (*Principles 2 and 6*)
- In view of the importance of effective communications during a *major operational disruption, financial industry participants* and *financial authorities* would be wise to anticipate that such disruptions might affect telecommunication systems. In-house telecommunications systems and wireless transmitters on buildings should have backup power. Redundant systems, such as analogue line phones and satellite phones, and other simple measures, such as ensuring the availability of extra batteries for mobile phones, may prove essential to maintaining communications in a wide-scale infrastructure failure. (*Principle 4*)
- Existing internal and external *communication protocols* were extremely useful in managing the domestic implications of the outage for the financial systems in the United States and Canada and facilitating and coordinating internal and external information flows between domestic *financial authorities* and the local emergency management officials responsible for the restoration of *physical infrastructure*. Nonetheless, *financial authorities* in both jurisdictions recognised following post-event reviews that further consultations on appropriate *communication protocols* would be useful to promote a common understanding of the type of disruption that might trigger cross-border communications and the nature of information that might be shared under such circumstances. (*Principles 4 and 5*)
- *Communication protocols* enabled *critical market participants* and their *financial authorities* to coordinate with local governmental emergency response organisations

and develop and implement “work-around” arrangements to maintain *critical operations*. (*Principle 4*)

- More work was needed to coordinate the numerous inter-agency and industry-wide conference calls with other conference calls involving several financial sector trade associations. As a result, a consolidated call matrix has been developed to better coordinate future emergency calls involving individual *financial authorities*, financial sector trade associations, and inter-agency working groups. (*Principle 4*)
- Maintaining lists of contact information for key officials would expedite consultations among *financial authorities* nationally and internationally in the event of an operational disruption. (*Principles 4 and 5*)

Annex II

Case study: The impact of the 2003 SARS outbreak on Hong Kong SAR's securities markets

Event

1. Hong Kong experienced a serious outbreak of SARS in 2003, the first major epidemic to affect the region in recent times. The outbreak originated with the arrival in late February 2003 of a carrier from mainland China and ended officially on 23 June 2003 when the World Health Organisation removed Hong Kong from the list of affected countries. Before the spread of the virus was arrested, the outbreak in Hong Kong would trigger similar outbreaks in Canada, Singapore and Vietnam.

2. The Hong Kong SARS outbreak was preceded by a similar outbreak in the neighbouring Guangdong Province of China. The local news media in Hong Kong were the first to report on the outbreak and spread of the disease, but little information about SARS was available in the early stages of the outbreak from the Chinese government, local health authorities or other official sources. As a result, rumours were rife in Hong Kong and anxiety was high until the outbreak was brought under control.

Impact

3. The 2003 SARS outbreak resulted in 1,755 cases and 300 deaths in Hong Kong alone. In addition to the tragic loss of life, the epidemic caused widespread fear and anxiety in the local community and had a significant impact on employment levels and the economy overall.

4. The Hong Kong securities industry did not experience major disruptions as a direct result of the outbreak. There was no serious spread of infection in the industry and the few individuals who were quarantined during the outbreak developed no sign of illness. Some of the measures introduced by the local *financial authorities*, brokerages and other market participants to slow the spread of the disease and the fear that permeated the local business community did affect the normal efficiency of day-to-day operations.

Response

5. At the time of the outbreak, Hong Kong's securities market encompassed more than 400 securities and 100 futures brokerages as well as hundreds of investment advisers, fund managers and other market participants. Although the global investment banks account for more than half of the turnover in the securities market today as they did then, the majority of brokerages (over 350) are local firms servicing the retail market. In addition to having to be licensed by the SFC, brokerages that trade in the securities, futures or options markets must be trading participants of HKEx, the parent company of the Stock Exchange of Hong Kong and the Hong Kong Futures Exchange.

6. The Hong Kong Securities and Futures Commission (SFC) is the frontline regulator for market intermediaries and the HKEx. All securities, futures and stock options transactions are electronically cleared and settled through clearing entities that are wholly owned subsidiaries of HKEx.

7. All relevant *financial authorities* and most brokerages and other relevant market participants, including the operators of securities clearing and settlement systems, implemented preventative measures to slow the spread of SARS, although not all at the same stage of the outbreak. For example, because of the shortage of reliable information in the initial stages of the outbreak about SARS and the extent to which it had spread in Hong Kong, it was not before the SFC learned of the preventative measures put in place by firms in the global investment banking community that SFC management created an internal task force on 26 March 2003 to deal with the internal and market impacts of the outbreak. HKEx created a similar internal task force and the two met daily to formulate policies and procedures, monitor their implementation, and track cases where market participants and SFC or HKEx staff or their families were affected.

8. The measures introduced by the relevant Hong Kong *financial authorities* to address the internal impacts of the outbreak varied from one organisation to another. They included the following:

- Notices were issued regularly to staff about the organisation's response to the outbreak and about how staff should proceed if they suspect they have become infected (ie inform management, seek medical attention and refrain from coming to work for the ten-day incubation period and thereafter until it is confirmed that they do not have SARS). Staff who became infected would be subject to strict quarantine procedures.
- A variety of approaches were taken to ensure a minimum level of service would be maintained if an organisation's offices were infected. Some organisations implemented a "split team approach" in which two teams were established from a group's existing complement, each of which was capable of backing the other up. At all times until the outbreak subsided, members of one of the two teams would work from home. In other organisations, redundancy was introduced by moving parts of teams to separate office locations for the duration of the outbreak. Telephone conference calls were encouraged in place of face-to-face meetings.
- Staff were given the option of cancelling non-essential meetings with external parties and on-site inspections were temporarily suspended. A casual dress code was introduced to facilitate the cleaning and disinfecting of clothing, and staff that were pregnant were asked to take early maternity leave.
- Face masks were distributed to all staff. When the local supply ran out, the SFC found alternative sources. Staff were encouraged to wear masks at all times, and those who were required to deal with the public were encouraged to wash their face and hands thoroughly with soap after meeting with external parties.
- Lavatories, elevators and public areas were cleaned hourly throughout the day, and offices were thoroughly cleaned and disinfected nightly. Arrangements were made for a team to disinfect and quarantine offices in the event of an outbreak.

9. The following actions were among those taken by the relevant Hong Kong *financial authorities* to address the potential market impacts of the outbreak:

- Circulars were sent to all market participants asking them to advise the relevant authority should any of their staff become infected and to ensure their *business continuity plans* were capable of responding to such an occurrence, and identifying

business continuity procedures of particular relevance to the outbreak. Relevant information from local health authorities was also circulated to all market participants.

- Exchange participants were notified of the steps that would be taken if it became necessary to suspend trading due to a confirmed case of SARS on the exchange trading floor. In particular, the trading floor would be closed 30 minutes after participants were notified of the event and would remain closed for the rest of the trading day for a thorough cleaning. It would only reopen with the approval of the health authorities or after a suitable quarantine period had elapsed.
- A database was set up to monitor the status of reported cases involving brokerages and other market participants.
- A hotline was staffed to answer questions from investors and other market participants about the outbreak and its effect on the local securities industry.

10. The members of Hong Kong's investment banking community shared information freely in a cooperative effort to minimise the spread of infection. Perhaps as a result, none of the staff at any of the major investment banks contracted SARS during the outbreak. Staff at the smaller retail brokers and other market participants also avoided infection during the outbreak. In addition to implementing many of the same measures that *financial authorities* introduced to address the internal impacts of the outbreak, the following strategies were employed by many of the brokerages and other market participants:

- Daily *business continuity* briefing meetings were held to discuss the latest developments. Staff were updated on the status of the outbreak and other relevant information via websites or daily e-mails.
- Some firms hired medical professionals to be available to staff in their offices during the day.
- Staff that would normally take public transport to work were reimbursed for taxi fares to minimise their exposure to higher risk areas. Flexible work hours were introduced so that those who did take public transport could commute outside of rush hours.
- Business travel in Asia was severely curtailed and otherwise restricted to essential trips, and policies were introduced that required senior management signoff for all business travel. In some firms, Hong Kong staff visiting offices in other locations were required to visit a doctor before leaving Hong Kong.

Lessons Learned

11. Although its impact on the Hong Kong securities industry was relatively minor, the 2003 SARS outbreak had the potential to cause a *major operational disruption* locally and, because of the significance of the Hong Kong financial market globally, affect the financial system in other jurisdictions. As the first event of its kind to affect Hong Kong in recent times, the outbreak was a true test of the *business continuity* management of *financial authorities* and participants in the securities industry. The following are some of the lessons that can be drawn from the experience:

- At the time of the outbreak, the SFC had a comprehensive market contingency plan for addressing disruptions that affect the markets and a *business continuity plan* to address disruptions of its own operations. These plans assumed implicitly that some staff would always be available in firms and at the SFC to maintain operations in the

event of a *major operational disruption*. SARS made it clear that that assumption is not always valid. The suspicion that one member of staff was infected would have been sufficient to cause an entire division to be quarantined and its operations to be shut down for at least ten days. Those plans nonetheless had to be revised during the outbreak to account for such impacts. (*Principle 2*)

- Implementing SARS-tailored contingency procedures was facilitated by established market contingency and *business continuity plans*. Although they did not explicitly consider scenarios in which no one would be available to continue operating a particular function or an entire business, these plans provided a useful framework for addressing the host of issues that arose from the outbreak. That the SFC and other organisations had *business continuity plans* in place and a structure for dealing with disruptions was clearly a factor in their ability to respond as effectively as they did. (*Principle 1*)

- Organisations can learn from the experience of others and adjust their *business continuity plans* accordingly. With the benefit of Hong Kong's experience to learn from, the *financial authorities* in jurisdictions to which the SARS virus spread all triggered their *business continuity plans* as soon as cases appeared within their borders. (*Principle 1*)

- Responding to a crisis in the absence of timely, complete and reliable information is particularly challenging. It affects management's ability to determine whether to trigger a *business continuity plan* and can contribute more generally to a sense of helplessness and anxiety, which in turn can exacerbate efforts to address the crisis. In such circumstances, effective internal and external communications are critical to ensuring senior management have access to all relevant information for decision-making purposes as soon as it becomes available, and to help staff make more informed decisions in their work and about matters that affect them and their families. Communication among *financial authorities*, market participants and the government proved essential to an organisation's awareness of the status of the outbreak and their ability to determine the appropriate course of action. (*Principle 4*)

- In the absence of established procedures and *communication protocols*, it is unlikely that *financial authorities* in the midst of a domestic operational disruption would be able to divert attention away from responding to the local situation to consider whether *financial authorities* in other jurisdictions should be contacted, who to contact, or how to reach them. This was the experience of Hong Kong authorities during the 2003 SARS outbreak. Because their time was fully absorbed addressing the local implications of the outbreak, there was no opportunity for Hong Kong *authorities* to initiate communications with *financial authorities* in other jurisdictions beyond occasional high-level status reports provided at meetings of various international standard-setting bodies. It was also the case that no foreign *financial authorities* initiated contact with their counterparts in Hong Kong to assess the potential impact of the Hong Kong outbreak on the financial system in their jurisdictions or learn from the steps taken in Hong Kong in the event the outbreak were to spread. (*Principle 5*)

Annex III

Case Study: The impact of the 2003 SARS outbreak on the Canadian securities industry

Event

1. The 2003 SARS outbreak in Canada was principally confined to the Greater Toronto Area in the province of Ontario. The outbreak developed in two waves, the first originating on 13 March 2003 and the second on 28 May 2003.

Impact

2. The Canadian securities industry did not experience major disruptions as a result of the 2003 SARS outbreak. A few individuals from within the regulatory or dealer communities were quarantined during the outbreak, but none of them developed signs of illness and there was no spread of infection within these communities. None of the relevant *financial authorities* or dealer firms reported an impact on their business operations, apart from minor disruptions arising from the need to redirect telephone and mail to staff working at *alternate sites*.

Response

3. The Canadian securities industry is concentrated, with the six largest integrated firms (all dealer affiliates of the major banks) generating about two-thirds of total industry revenues. Geographically, the largest capital markets are located in Ontario. The responsibility for regulating the Canadian securities industry is shared by provincial authorities. In addition to the provincial regulatory authorities, most dealers are members of one of the self-regulatory organisations (SROs) with responsibility for enforcing market integrity rules and otherwise regulating the trading of equities and fixed income securities in Canada. Some dealers are integrated firms, whereas others focus on a specific market segment, such as institutional or retail. Securities trades are cleared and settled by a Canadian clearing agent offering electronic clearing services both domestically and internationally.

4. The responses of the relevant *financial authorities* and *financial industry participants* to the SARS outbreak varied. The provincial regulatory authority in Ontario identified the outbreak as a market disruption issue and proceeded to monitor market participants' reactions to it. Some *financial authorities* arranged to share office space and access to technology with one another, agreed on reciprocal arrangements for workload sharing with other *authorities*, and made special arrangements with vendors to run some of their processes externally.

5. More generally, the responses of the relevant *financial authorities* and *financial industry participants* included some or all of the following actions:

- Organising meetings of the board and senior management, both at the onset of the outbreak and thereafter as necessary, to identify the risks to their organisation and assess appropriate measures for addressing them. The main risk identified by most organisations was the inability to continue operating key parts or all of their business as a result of the infection or extended quarantine of staff;
- Establishing "clean teams" for certain functions in *alternate sites* or creating isolated groups by temporarily relocating staff from certain functions to different floors of the same building;
- Restricting access to business facilities to specified staff, enabling staff to work from home, encouraging the use of conference calls and other alternatives to face-to-face meetings, and in some cases advising staff to remain out of the office;
- Restricting travel to, and mandating quarantine for staff returning from, high-risk areas and temporarily suspending certain activities in order to minimise the risk of external contact;
- Creating additional communication lines and communicating regularly with staff to educate (eg by circulating advisories from public health authorities) and update them on SARS-related developments via notices on websites or call-in information lines, and advising staff to notify managers and seek appropriate medical attention if they experienced SARS-like symptoms or had reason to believe that they may have been exposed to SARS; and,
- Promoting simple measures to prevent contamination, such as exercising utmost care in their contacts, washing hands (some organisations made hand sanitizer available), and avoiding sharing PC peripherals and phones.

Lessons learned

6. Because the outbreak ultimately had only a limited impact on the Canadian securities industry, the responses of *financial authorities* and market participants were almost all of a preventative nature. Nonetheless, it is possible to draw from the experience the following lessons applicable to the management of *business continuity*.

- The impact of the event was limited even though the responses of individual *financial authorities* and *financial industry participants* to the outbreak varied. Each determined its course of action based on the organisation's assessment of its relative position in the Canadian securities industry and the nature of the functions it performed. (*Principle 3*)
- At the time of the outbreak, the *business continuity plans* of most organisations had not explicitly considered scenarios where there may be insufficient staff to conduct business due to illness or quarantine. It soon became clear as the health crisis unfolded that the possibility of a single employee being exposed to the virus could affect the operation of an entire business function in both its primary and *alternate sites* – and possibly for an extended period of time. On the basis of this experience, organisations have updated and modified their *business continuity plans* to incorporate scenarios involving significant risk to life and property irrespective of the cause, whether force of nature, accident, or intentional act. (*Principle 2*)
- The boards and senior management of organisations involved in the Canadian securities industry acted early in the crisis to identify the risks to their employees as well as the organisations. A variety of steps were taken to minimise the risk that employees would be exposed to the SARS virus, including educating staff about the

virus and how it is spread. The swift response and the nature of the steps taken may well have prevented a more serious outcome. (*Principle 1*)

- The relevant *financial authorities* and *financial industry participants* have recognised the importance of regularly updating *business continuity plans* and have done so on the basis of their experience with the SARS outbreak. In particular, a number of organisations have taken steps to address certain limitations in their *alternate site* arrangements, such as the number of workstations and communication devices. (*Principle 2*)
- The time for addressing an organisation's communications requirements under stress conditions is not during an actual disruption but when markets are operating normally. The communication challenges during the SARS outbreak revolved mainly around the ability to communicate with staff spread out over multiple locations away from the primary business location (eg at *alternate sites* and in their homes) about developments with the outbreak and business-related matters. (*Principles 4 and 5*)

Annex IV

Case study: Niigata Chuetsu earthquake

Event

1. The Niigata Chuetsu earthquake, measuring 6.8 on the Richter scale and affecting the Chuetsu region of Niigata prefecture, occurred at 17:56 local time on 23 October 2004. It was followed by a series of aftershocks that continued for two months.

Impact

2. The earthquake caused significant damage to *physical infrastructure* and buildings. Its impact on the financial system and overall economy was minor, however, in relation to the impact of events like 11 September 2001 and the Hanshin-Awaji earthquake that struck Kobe and Osaka on 17 January 1995. The impact was relatively minor because the earthquake occurred in a rural area on a Saturday, which provided a two-day window for steps to be taken before banking transactions would resume on the following Monday.

3. The destruction of *physical infrastructure* and buildings presented the most significant impediment to the ability of financial institutions to continue operating. In particular, transporting employees, cash, bills and checks, mail, and other goods became difficult, and accommodating employees who had been displaced from their homes or offices proved challenging. Some branches were forced to close temporarily due to structural damage, and some off-premise ATMs became unavailable. Evacuation advisories caused some financial institutions to suspend operations.

4. Most of the financial institutions operating in areas affected by blackouts were able to continue operating on backup power supplies, and quake-absorbing construction techniques enabled their computer centres to withstand the impact. Communication lines for ATMs and other services generally functioned without problems. Facility damage at financial institutions was minor, largely due to measures that were implemented to provide protection from lightning strikes but which also contributed to the ability to withstand earthquakes and *business continuity plans* whose development was based on the experience of the Hanshin-Awaji earthquake.

Response

5. The Ministry of Finance and the Bank of Japan assessed the condition of the quake-stricken areas and confirmed that the Disaster Relief Law was applicable in light of the nature and extent of physical damage in the region. In response, local public authorities take steps to provide shelter and other services to victims of the disaster.

6. Japanese *financial authorities* subsequently directed financial institutions to implement “Financial Measures Associated with Earthquake Damage”, special measures designed to minimise an earthquake’s impact on individuals in the affected areas. The measures include, for example, provisions directing banks to release funds where a deposit

certificate or passbook is lost and replace dirty, torn or otherwise mutilated money and insurance companies to pay insurance benefits promptly and extend moratoria on premium payments.

7. Because of the heavy volume of calls experienced by telephone carriers in the aftermath of the earthquake, it took some time before *financial authorities* were able to communicate with financial institutions in the affected areas. However, the telephone numbers that financial institutions and *financial authorities* had shared previously for contact outside of normal business hours proved helpful.

8. Japanese authorities implemented an emergency calling tree that included the relevant domestic authorities, such as the Cabinet Office, Ministry of Finance, Bank of Japan, Financial Services Agency, Disaster Countermeasures Office of Niigata Prefecture, Niigata Prefectural Government and a number of industry organisations. Most authorities used a priority telephone service in the initial stage of the response, while a central wireless system was used for communication between the Cabinet Office and other relevant authorities.

9. Most financial institutions were able to confirm the safety of their employees and ascertain the nature and extent of damage to their facilities by the day following the quake. Others, however, had difficulty confirming the status for a few days afterward. Financial institutions were asked to report to the Niigata Finance Office and the Bank of Japan (Niigata Branch) on the damage they had incurred and whether they were capable of operating.

10. Before the earthquake, many of the businesses operating in the Chuetsu region of Niigata prefecture had well-developed policies requiring backup power sources and lines to cope with the frequent lightning strikes in the region. Consequently, more than 90% of the retail premises operated by regional banks in Niigata have their own power generating facilities.

11. Financial institutions used alternate routes to transport cash in the areas where the transportation infrastructure was severely damaged. Some had cooperative schemes with other financial institutions that enabled prompt cash delivery to their partners. Although financial institutions in Japan are normally closed on weekends, many in the region affected by the earthquake opened on weekends and introduced low-interest loan facilities to meet the special needs of customers in the region.

12. When an earthquake occurs in Japan, insurance companies are required to handle associated claims (ie claims under policies covering fire and earthquake damage) expeditiously and make the operation of their service centres (regional offices responsible for processing claims) their highest priority. Consequently, they have developed *business continuity plans* with an emphasis on service centre operation and were able to deal effectively with large-scale loss inquiries and insurance payments and draw upon their high level of liquidity to cover claims in response to the Niigata Chuetsu earthquake.

Lessons learned

13. The lessons learned from the Niigata Chuetsu earthquake include the following:

- There was minimal interruption in the services provided by financial institutions affected by the earthquake largely because their *business continuity plans* incorporated the lessons learned from the Hanshin-Awaji earthquake and from the frequent lightning strikes in the region. (*Principles 1 and 2*)

- Explicitly addressing the possibility of disruptions to telecommunication, power, gas, water and transport systems in areas affected by earthquakes and other natural and man-made events in *business continuity plans* improves an organisation's *resilience* to such disruptions and ability to recover from them. Many financial institutions in the affected region found that pre-arranged cooperative service arrangements with other financial institutions can be particularly helpful in maintaining service during a disruption. (*Principle 2*)
- Public confidence in the financial system was maintained following the Niigata Chuetsu earthquake because of the ability of financial institutions in the region to withstand and recover quickly from the event. Clients of financial institutions in the region experienced minimal interruption in their access to retail financial services. (*Principle 3*)
- Access to a variety of communication channels and off-hour contact information is beneficial in efforts to coordinate responses to a *major operational disruption* among financial institutions and relevant authorities. *Communication protocols* that were available to all relevant organisations and included key contact information proved helpful in responding to the earthquake. (*Principle 4*)
- Financial institutions in the Chuetsu region were accustomed to testing their backup power supplies and evacuation procedures at least annually, which contributed to their *resilience* to this disruption. (*Principle 6*)

Annex V

Case Study: The London terrorist attacks on 7 July 2005

Event

1. On 7 July 2005 three widely-dispersed explosions occurred in the London Underground at approximately 8:50, followed an hour later by a fourth explosion on a bus in Tavistock Square. All four explosions were later confirmed as suicide bombings – the first such attacks in the United Kingdom. More than 50 people were killed and 700 injured in the explosions. For a significant period the public transportation system in London was at a complete standstill.

Impact

2. The attacks, although tragic in terms of the loss of life and injuries, did not directly target the financial sector and thus had little overall impact upon the financial system. Nevertheless there was indirect impact in terms of disruption to travel arrangements, communications and access to property within exclusion zones, which presented the sector with a number of challenges.

3. The financial markets proved to be resilient, although the volume of order book trading reached record levels during 7 July.

Response

4. Most providers of *critical services* experienced low levels of physical disruption, although one was obliged to relocate to its *alternate site*. It was nonetheless able to maintain normal service throughout. Several others made adjustments to their normal operating systems to cope with the higher than usual volumes of trade and in response to localised shortages of personnel. These arrangements were successful.

5. To ensure that the market remained orderly in the face of record trading volumes on 7 July and that market participants' systems were able to manage the higher trading volumes, the London Stock Exchange declared a 'fast market' (under which certain obligations on market makers are lifted) and suspended the use of Automated Input Facilities (commonly known as "black box" trading) which account for the majority of orders placed on the order book. These restrictions were lifted before the closing auction, however, which went smoothly.

6. Although few firms were directly affected by the events, many activated their *alternate sites*, for the most part as a precautionary move.

7. The UK *financial authorities* were not themselves significantly affected by the incident and were able to invoke their collective response arrangements at an early stage. These consisted mainly of contacting *financial industry participants* to assess the extent to

which they had been affected by the events and, on the basis of that information, to make an overall judgement on whether the financial sector was at risk of substantive disruption.

Lessons Learned

8. To more accurately gauge the impact of the events on the financial sector and the financial sector's response, the UK *financial authorities* conducted a survey of major financial institutions immediately afterward. It was clear from their responses that several important lessons had been learned, as summarised below.

- A number of financial institutions who activated their *alternate sites* expressed concern about the ability of the providers of syndicated backup facilities to meet firms' needs if faced with a wide-area event. In addition, there is some concern about the level of syndication of individual sites with particular uncertainty about the criteria that providers apply for prioritisation and space sharing. (*Principle 2*)
- Overall, most financial institutions believed that their *business continuity plans* had served them well on the day and had been sufficiently flexible to adapt to the nature of the incident. It appears that *business continuity planning* in many financial institutions is focussed upon impact and decision-making processes rather than on the nature of the disruption. This gives them what they perceive to be greater flexibility in responding to a broad range of potential scenarios. This generic impact-based approach worked particularly well for those financial institutions whose key staff had clearly defined roles and responsibilities that they had rehearsed and for which they had been well trained. (*Principle 2*)
- Most financial institutions that responded to the post-event survey were satisfied with the level of direct contact and support they received from the relevant authorities. However, most indicated that they would have appreciated more communication from the *financial authorities* during the course of the day on the status of the various financial markets. (*Principle 4*)
- A majority of financial institutions identified at least a few areas where communications within their organisations could be improved. Congestion and subsequent disruption to the mobile telephone networks was cited as the main obstacle to effective communication, although this did not appear to have had a significant impact upon principal business activities. Almost all financial institutions surveyed indicated that they intend to make some changes to their *business continuity plans* as a result of the difficulties they experienced. In particular, this is likely to be aimed at improving fallback arrangements should the main communications technology prove unreliable during an event. (*Principle 4*)
- In terms of monitoring the unfolding of the incident, the satellite news media were reported to have been the most valuable source of up-to-date information. However, nearly half of the financial institutions surveyed reported that their crisis management teams did not have direct access to this media. This meant in a number of cases that staff with direct access had more current information than the crisis management team. There was a general perception that official news channels at times lagged behind media reports, although it should also be recognised that official announcements require more thorough validation. (*Principle 4*)
- Data networks remained largely unaffected but the surge in e-mail traffic during the incident slowed delivery and access to the internet was similarly affected. (*Principles 4 and 6*)

- Financial institutions made people their main priority. However, as might be expected this proved to be the most challenging aspect of responding to events, particularly in view of the shutdown in public transport and the congestion on mobile phone networks. (*Principles 1, 2 and 3*)
- The timing of the incidents meant that most financial institutions' staff were already at or close to work before the disruption began. Consequently, unscheduled absence of key staff was not a significant feature of the event. However, many financial institutions experienced difficulties in accounting for staff on the move and it is clear that there is enormous variation in the methods for doing so. Most financial institutions had nonetheless accounted for all of their staff within three hours. More challenging for many was the task of accounting for visitors and contractors, with only around half being able to do so with a high level of certainty. (*Principle 4*)
- A majority of financial institutions took a proactive approach to ensuring the welfare of their staff. Few firms had formal contingency plans in place, however, and ad hoc arrangements proved challenging. Several financial institutions noted that there was insufficient information provided by the authorities on the overall coordination of plans for transport and evacuation during the course of the day. This meant that individual financial institutions lacked a context in which to set their own plans. (*Principle 6*)
- Many financial institutions advised non-essential staff to remain at home on the day following the incidents mainly because they recognised that the transport system would still be disrupted. Many staff were able to use remote access technology to work from home. Nonetheless, a few financial institutions experienced unscheduled staff absences of above 20% – no doubt reflecting staff concerns about the risk of further incidents. (*Principle 3*)
- The events of 7 July 2005 have reaffirmed the priority assigned by UK *financial authorities* to regular market-wide testing and to benchmarking the *resilience* of the UK financial sector. (*Principles 6 and 7*)
- Communication with foreign *financial authorities* and *financial industry participants* during the events of 7 July 2005 was initiated principally by foreign organisations and was generally low-key and ad hoc. This was because the UK *financial authorities* had ascertained at an early stage that the events posed no significant threat to the UK financial sector and thus no risk of cross-border ramifications. Nonetheless, the UK *financial authorities* are reviewing their *communication protocols* in the light of this recent experience. There may be room for such protocols to consider the circumstances in which the *financial authorities* in a jurisdiction affected by a *major operational disruption* should be the ones to initiate communications with *financial authorities* and *critical market participants* in other relevant jurisdictions. These circumstances would include, in particular, disruptions with the potential of cross-border implications where *financial authorities* in other jurisdictions are likely to know that a disruption has occurred. (*Principle 5*)

Annex VI

Bibliography

Australian Prudential Regulation Authority (2005): *Guidance note AGN 232.1 (Authorised Deposit-Taking Institutions) and GGN 222.1 (General Insurers), Risk assessment and business continuity management*, April, http://www.apra.gov.au/Policy/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=8529, and http://www.apra.gov.au/General/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=8532.

- - - (2005): *Prudential standards APS 232 (Authorised Deposit-Taking Institutions) and GPS 222 (General Insurers), Business continuity management*, April, http://www.apra.gov.au/Policy/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=8528, and http://www.apra.gov.au/General/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=8531.

Banca d'Italia (2004), *Continuità operativa in casi di emergenza (Regulation on Business Continuity Management),* Bollettino di Vigilanza, pages 7-13, July*,* http://www.bancaditalia.it/vigilanza_tutela/vig_ban/pubblicazioni/boll_vig/anno04/bolvig_07_04.pdf#page=11.

Bank of Japan (2003): *Business continuity planning at financial institutions*, July, http://www.boj.or.jp/en/set/03/fsk0307a.htm.

- - - (2003): *Business continuity planning at the Bank of Japan*, September, http://www.boj.or.jp/en/about/03/sai0309a.htm.

Banque de France (2004): *The resilience of post market infrastructures and payment systems*, Revue de la stabilité financière, pages 107-114, November, http://www.banque-france.fr/gb/publications/rsf/rsf_112004.htm.

Committee on Payment and Settlement Systems (2001): *Core principles for systemically important payment systems*, January, http://www.bis.org/publ/cpss43.htm.

- - - / International Organization of Securities Commission (2001); *Recommendations for securities settlement systems*, November, http://www.bis.org/publ/cpss46.htm.

Commission of the European Communities (2005): *Green paper on a European programme for critical infrastructure protection*, November, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

De Nederlandsche Bank (2004): *Assessment framework for BCP in respect of payment and securities settlement systems,* http://www.dnb.nl/dnb/bin/doc/Assessment%20framework_tcm13-49071.pdf.

European Central Bank (2001): *Memorandum of understanding on co-operation between payment systems overseers and banking supervisors in stage three of economic and monetary union*, http://www.ecb.int/press/pr/date/2001/html/pr010402.en.html.

- - - (2003): *Memorandum of understanding on high-level principles of co-operation between banking supervisors and central banks of the European Union in crisis management situations*, http://www.ecb.int/press/pr/date/2003/html/pr030310_3.en.html.

- - - (2005): *Memorandum of understanding on co-operation between the banking supervisors, central banks and finance ministries of the European Union in financial crisis situations* (2005), http://www.ecb.int/press/pr/date/2005/html/pr050518_1.en.html.

- - - (2005): *Payment systems business continuity – issues paper*, http://www.ecb.int/ecb/cons/previous/html/paysysbusinesscontinuity.en.html.

Federal Financial Institution Examination Council (2003): *IT handbook on business continuity planning*, http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.

The Federal Reserve Board, the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission, United States of America (2003): *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/default.htm.

Financial Services Authority, United Kingdom (2003): *BCM risk matrix,* http://www.fsc.gov.uk/upload/public/attachments/6/bcmriskmatrix.pdf*.*

- - - (2002): *Operational risk systems and control, UK FSA consultation paper #142*, http://www.fsa.gov.uk/pubs/cp/cp142.pdf*.*

- - - (2002): *A risk-focused review of business continuity management in major financial groups post September 11*, http://www.fsc.gov.uk/upload/public/Files/1/fsa_bcm_paper_2002-09.pdf*.*

Financial Stability Committee, Belgium (2004): *Financial Stability Committee recommendations on business continuity planning*, http://www.cbfa.be/eng/aboutcbfa/cfs/pdf/business_continuity_planning.pdf.

Hong Kong Monetary Authority (2002): *Supervisory policy manual ("SPM") TM-G-2: business continuity planning*, December, http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-G-2.pdf.

Monetary Authority of Singapore, (2003): *Business continuity management guidelines*, http://www.mas.gov.sg/regulations/download/BCMGuidelines.pdf*.*

Summary of "lessons learned" from events of September 11 and implications for business continuity (2002), http://www.sec.gov/divisions/marketreg/lessonslearned.htm.

Task Force on Major Operational Disruption in the Financial System, United Kingdom (2003): *Do we need new statutory powers? Report of the Task Force on Major Operational Disruption in the Financial System*, http://www.bankofengland.co.uk/publications/other/financialstability/taskforce/index.htm.

Tripartite Standing Committee, United Kingdom (2004): *Financial sector business continuity progress report*, http://www.fsc.gov.uk/upload/public/Files/1/Report.pdf*.*

Annex VII

Members of the Joint Forum Business Continuity Working Group

Chairman:	**John Sloan (UK FSA)**
Australia:	Heidi Richards (APRA)
Canada:	Judy Cameron (OSFI) Randee B. Pavalow (OSC)
France:	Alain Dequier (Commission Bancaire)
Hong Kong SAR:	Angelina Kwan (Securities and Futures Commission)
Japan:	Ei-ichiro Fukase (Bank of Japan)
The Netherlands:	Rick Angevaare (DNB)
UK:	John Milne (FSA)
USA:	Angela Desmond (FRB) Alton Harvey (SEC) Mike Yuenger (OCC)
CPSS liaison:	Benjamin Hanssens (CPSS Secretariat)
Secretariat:	Jeff Miller (Joint Forum Secretariat)