20 Questions

Directors Should Ask about the Information Technology Aspects of Business Continuity Planning

The Canadian Institute of Chartered Accountants

How to use this publication

Each “20 Questions” briefing is designed to be a concise, easy-to-read introduction to an issue of importance to directors. The question format reflects the oversight role of directors, which includes asking management — and themselves — tough questions. The questions are not intended to be a precise checklist, but rather a way to provide insight and stimulate discussion on important topics.

The comments that accompany the question summarize current thinking on the issues of leading organizations and provide directors with a basis for critically assessing the answers they get and digging deeper as necessary. Thus, although the questions apply to most medium- to large-sized organizations, the answers will vary according to the size, complexity and sophistication of each individual organization.

The Information Technology Advisory Committee

The Canadian Institute of Chartered Accountants

20 Questions

Directors Should Ask about the Information Technology Aspects of

Business Continuity Planning

The Canadian Institute
of Chartered Accountants

Library and Archives Canada Cataloguing in Publication

20 questions directors should ask about the information technology aspects of business continuity planning.

ISBN 1-55385-172-2

1. Business enterprises — Computer networks — Security measures. 2. Information technology — Security measures. 3. Computer security. 4. Information resources management. I. Canadian Institute of Chartered Accountants. II. Title: Twenty questions directors should ask about the information technology aspects of business continuity planning.

HD61.T84 2005 658.4'78 C2005-904180-3

Printed in Canada
Disponible en français
www.icca.ca/ccti

Preface

The CICA's Information Technology Advisory Committee developed this brochure to guide the members of boards of directors in evaluating the information technology aspects of business continuity planning issues that might arise while they discharge their board responsibilities. This document might also be of interest and use to members of other governance bodies — in particular audit committees and strategic bodies such as IT steering committees.

Directors of organizations are expected to satisfy themselves that the information technology function is effective, and that it provides the organization with sound business continuity strategies and plans. This brochure proposes questions for boards to ask the Chief Information Officers and others. For each question there is a brief explanatory background. We hope that directors, CEOs and CIOs will find it useful in assessing their approach to the management of risk and internal control.

The CICA would like to express its gratitude to the principal author of this brochure, Carole Le Néal, CISA, CISSP, CIA, a member of the Information Technology Advisory Committee, and to the other members of this Committee for their advice and comments.

Board Responsibilities for Business Continuity Planning

The need for reliable business continuity and disaster recovery and response plans (BCP/DRP)[1] has been extensively discussed and written about ever since organizations first began to automate some of their manual data processing systems. Formalized or not, however, business continuity planning is and always has been a business issue for owners, shareholders, customers, employees, suppliers, regulators and the community at large. Survey after survey has shown that business continuity planning remains among the top concerns of business leaders and IT professionals around the world.

This is hardly surprising given the fact that no matter how well prepared organizations consider themselves to be, unanticipated types of disasters reveal shortcomings in the risk scenarios upon which their BCPs are based. Major events, such as Eastern Canada's Ice Storm of 1998, the 9/11 terrorist attacks of 2001 on New York's World Trade Center, Eastern North America's Great Blackout of August 2003, and the Asian Tsunami of December 2004, immediately come to mind. However, increasingly frequent service interruptions resulting from more common occurrences, such as the spread of computer viruses, errors during minor changes to information systems or technological infrastructures, or one-day strikes by critical IT personnel, demonstrate the need for companies to continually review their business continuity and response plans in order to quickly restore essential services.

This brochure focuses on issues that need to be addressed as part of the organization's overall business continuity plan in order to ensure the continuous availability or rapid recovery of its critical information systems and services.

---

[1] The term Business Continuity Plan (BCP) "refers to the process of developing advance arrangements and procedures that enable an organisation to respond to an interruption in such a manner that critical business functions continue with planned levels of interruption or essential change. In simpler terms, BCP is the act of proactively strategising a method to prevent, if possible, and manage the consequences of a disaster, limiting the consequences to the extent that a business can absorb the impact." The Disaster Recovery Plan (DRP), a key component of BCP, refers to the technological aspect of the plan, while BCP addresses the overall operational and business aspect. (SOURCE: Information Systems Audit and Control Association (ISACA), *IS Auditing Guideline, Business Continuity Plan (BCP) Review from IT Perspective* (Document G32), 2005) Disaster Recovery Planning, or "Contingency Planning," can also be defined as "a process of preparation for the replacement of information systems following a disaster." (SOURCE: Deloitte & Touche and the Information Systems Audit and Control Foundation (ISACF), ISACF Board of Trustees, ISACF Research Board, *e-Commerce Security — Business Continuity Planning*, 2002, page 3) The Business Continuity Institute defines Business Continuity Management (BCM) as "An holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities." (see http://www.thebci.org/Glossary.pdf); its meaning is similar to that of Business Continuity Planning.

Governance Issues

In today's highly integrated economy, a majority of companies, both large and small, rely heavily on information technology to conduct their everyday business. Organizations communicate with their employees, branches, customers, distribution channels, supply chain, counterparts and the general public through e-mail, web-based services, electronic payment systems and on-demand access to corporate data. Numerous interfaces link critical corporate systems to internal and external sources of data. Just-in-time manufacturing processes require the continuous availability of ERP and electronic ordering systems to ensure the timely availability of parts. Hence, organizations can be severely affected by breakdowns in either their own systems or processes, or in those of critical business partners upon whom they depend.

The aftermath of the 2001 World Trade Center attacks has revealed just how sensitive national economies have become to the systemic risk resulting from these numerous interdependencies. Consequently, governments and regulators around the world have taken steps to protect industries and the general public. Industry-specific standards have emerged when the common good depends on the readiness of all service providers within that type of business. For example, the Federal Reserve System's April 2003 "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" and business continuity and contingency plan rules for the securities industry, adopted in 2004 by the Securities and Exchange Commission (SEC), the New York Stock Exchange (NYSE) and the National Association of Securities Dealers (NASD), led to the adoption of similar though less stringent standards by the Investment Dealers of Canada (By-law No. 17.19), and to the development of rules that are being considered by the Montreal Exchange and several provincial securities commissions.

Board members must therefore ensure that the organization's business continuity strategies are in keeping with its corporate policies and risk management strategies as well as with regulations and best practices. To discharge this responsibility, board members should seek answers to the following questions:

1. **Has the organization adopted a business continuity policy that defines management's responsibilities regarding the development, testing and maintenance of an effective business continuity plan for its critical services, business functions, systems and processes?**
2. **How has management ensured that formal responsibility for planning, coordinating and supporting the organization's BCP efforts is harmonized with its IT Security and Enterprise Risk Management functions?**
3. **Have adequate funding and resources been provided to develop and maintain the organization's business continuity plan?**
4. **What mechanisms have been implemented to ensure that the organization's business continuity plan complies with changes in industry practices, as well as with the laws and regulations governing the organization, both domestically and internationally?**

Risk Assessment and Mitigation

In order to develop an effective business continuity plan, the organization must first identify its threat environment and the financial and operational impacts of the risks to which it is exposed. Given the high level of integration and the complexity of today's information systems and infrastructures, both internal and external threats must be considered, including threats resulting from changes brought about during routine maintenance and risks arising from major projects. In certain industries, even a few hours of downtime can impact significantly on a company's operations, customer relationships, revenue and image. Awareness of the consequences of various types of contingencies allows the organization to determine the extent of the damage it has the capacity to absorb, and yet remain in business. Hence, it is important for executive management to implement effective mechanisms to ensure the periodic review of its risk assessments, risk scenarios, business impact analyses and key recovery time frames, as well as the regular testing and updating of its business continuity plan.

Surveys show that smaller and midsize companies tend to be ill prepared to deal with business disruptions. Yet they often depend even more heavily on uninterrupted access to their systems, data and supplies than larger organizations, whose systems, processes and workforce are generally more resilient.

BCP-related regulation will increase the expectations of various stakeholders, including customers and stockholders, in the continued operation of the business in the event of a contingency. Directors and officers who have not taken appropriate steps to ensure that the organization has a reliable business continuity plan thereby expose themselves to legal action should any of its stakeholders suffer material damage resulting from such negligence.

The results of the organization's risk assessment and business impact analyses will also allow it to evaluate the adequacy of its disaster insurance. Given their increasing dependency on e-commerce, and the enhanced risk environment in which they operate, companies should ensure that their insurance coverage includes protection against e-commerce risks and terrorism, as well as for operational losses resulting from material damages due to system failures. If management has outsourced critical business functions to external service providers, the organization's contracts with these business partners should require them to obtain similar coverage.

Here are the questions that board members should ask regarding these matters:

5. **How do business continuity plans reflect the results of the financial and operational risk assessments used to analyze the organization's exposure to various types of threats and vulnerabilities?**
6. **Have realistic risk scenarios been considered in the formulation of the organization's business continuity plan?**
7. **How does management ensure the plan is reliably updated to reflect changes to the organization's business and operational risks?**
8. **How does the organization ensure that its insurance coverage remains properly aligned with its evolving risk profile?**

Outsourcing Issues

Outsourcing presents a particular challenge to organizations that have transferred responsibility for managing key parts of their information technology environment to external service providers. Executive management must ensure that its contracts and/or service level agreements clearly define the outsourcers' responsibilities with respect to BCP. In order to protect its critical data, information systems, and infrastructure, the organization's contracts must require external service providers to comply with its policies, standards, procedures and other BCP requirements.

Security requirements must be clearly defined in outsourcing contracts. Should a contingency situation arise, the organization must, for example, have physical and logical access to its critical files. It must also be sure that software licences have been obtained for all sites where its critical information systems are likely to be processed, especially when the disaster recovery plan hinges on reciprocal agreements.

Finally, it is essential that rigorous reporting mechanisms, performance indicators, joint testing exercises, assurance reports on service organizations, and right-to-audit contract clauses enable the organization to effectively monitor critical service providers' compliance with its BCP requirements.

Board members should ask executive management:

9. **How clearly do contracts and/or service level agreements define service providers' responsibilities with respect to the organization's BCP, and enable the organization to monitor compliance?**

Human Resource and Communication Issues

Time and again, experience has shown that people issues are among the most delicate to handle in the event of a major disruption to an organization's critical business services. The astuteness with which a company plans and carries out its responsibilities towards its employees and others with a stake in the continuity of its operations can have a major impact on its reputation and, in extreme cases, on its very ability to survive.

Business continuity plans must define the measures needed to deal with the impacts of service disruptions on key personnel. The availability of information technology professionals, in particular, is essential to the timely recovery of critical information systems and to providing decision-makers with the information they need to manage such incidents. IT professionals are often required to work extra hours, at a time when their families may also need support. Measures must therefore be taken to ensure, for example, that alternates have been trained for critical functions, that proper compensation is given and that employees' family responsibilities are taken into account. Outsourcing contracts require similar action from critical external service providers. Unionized companies must identify, in the BCPs, the means required to maintain essential services in the event of a strike.

How well an organization communicates with the media, employees, customers, external service providers, peers and regulators in the event of a serious business disruption has a significant impact on stakeholders' confidence and, indeed, on the company's very reputation. Effective communication procedures and clear lines of responsibility can enhance public confidence in the organization and its management. Policies and a reliable escalation process, documented from the incident's detection to its ultimate resolution, are essential. Executive management's active involvement throughout the incident's life cycle provides stakeholders with the assurance they need that matters are, indeed, in good hands.

Here are the questions that board members should ask regarding these matters:

10. **What measures has the organization taken to inform and protect its employees as well as to ensure that key expertise remains available in the event of a disaster?**
11. **How does executive management ensure that communications with the media and key stakeholders are duly approved and conveyed through the proper channels?**
12. **Are the organization's incident response plans flexible enough to enable it to respond rapidly and appropriately to various types of interruptions to its critical operations?**

Change Management

Companies' heavy dependence on information technology, the complexity of today's applications and the high degree of integration among internal and external systems have highlighted the critical importance of rigorous change control and problem management procedures. Numerous incidents have shown the embarrassing effects of inadequate testing of even minor changes to software, hardware or the information technology control environment on the continuity of essential business services or functions. Effective controls are essential to ensure that even minor corrections required for troubleshooting or maintenance are performed in accordance with policies and procedures, and that these changes are reflected in the company's disaster recovery plan.

Experience has shown that system development projects can pose a business risk, especially when major changes are made to complex, highly integrated applications such as Enterprise Resource Planning systems (ERPs). Unanticipated effects of newly developed software can sometimes result in a major disruption to the organization's critical services, processes and functions. It is therefore essential that project plans include the development of contingency measures, designed to mitigate the commercial risks of software changes. This requirement should be part of the organization's project management methodology and reviews.

Here are the questions that board members should ask regarding these matters:

13. **What process has been implemented to ensure that the organization's disaster recovery plan is systematically updated and tested whenever major enhancements or routine maintenance are made to its critical information systems and infrastructures?**

14. **How does management ensure that plans to mitigate the risks, to its critical operations, of changes made to complex, highly integrated systems, are developed for all major projects?**

Tactical Considerations

The development of a reliable business continuity plan requires intimate knowledge of the organization's inner workings, including the links between the various business units, staff functions, data, information systems, processes and external relationships. Executive management responsible for critical business processes must be held accountable for ensuring that its part of the business recovery plan evolves in accordance with all significant changes to operations or to external needs.

Disaster recovery planning for critical systems and data is a key part of the business continuity plan. Business processes often rely on its 24/7/365 availability. Yet, surveys indicate that many small to medium-sized companies do not have adequate backup data and system recovery strategies, even though these requirements are critical to the organization's disaster recovery efforts. As data storage requirements explode, companies need to consider the use of data replication technology and strategies to distribute data over two or more geographically distant sites. A data storage, backup and restore architecture based on data mirroring and load balancing among multiple data centres enables IT-sensitive organizations to provide essential services more quickly when operations are interrupted at one of its critical sites.

As data, technologies, information systems and processes evolve, the organization must continually update its BCP to ensure that it remains current. Establishing the plan's reliability and effectiveness requires rigorous testing whenever significant changes are made to the company's information technology, operations, internal structure, location or business environment. Compliance with data privacy and confidentiality requirements must be ensured throughout the testing process.

Here are the questions that board members should ask regarding these matters:

15. **What alternatives to the organization's regular way of doing business have been developed to ensure the resiliency of its most critical data, systems, business functions, services and processes?**

16. **What steps have been taken to minimize the exposure of key personnel, and critical business and IT operations, to major crises?**

17. **How does management identify and protect the data and documents required to restore critical business services or functions in the event its contingency plans need to be activated?**

18. **Is the effectiveness of the organization's business continuity strategy regularly tested in compliance with corporate policy, or whenever significant changes alter its own technology, processes, structure, regulatory context or business environment, or those of its external service providers?**

Monitoring

Ensuring the availability of a reliable business continuity plan can only be achieved through the sustained leadership, sponsorship and commitment of the most senior levels of management. Hence, responsibility for defining business continuity objectives, and for monitoring compliance, must remain with executive management; it cannot be delegated to individual business units. Furthermore, management must be held accountable, through appropriate means, for ensuring the reliability of the business continuity plan specific to the critical business functions or services under its direct responsibility.

Events that disrupt the operations of other companies, both inside and outside the organization's industry sector, can provide early warning of the evolving threat environment. Internal incidents may reveal weaknesses in the organization's systems, processes and internal control environment. It is therefore essential for both directors and executive management to implement reliable methods for monitoring the effectiveness of risk mitigation strategies and the business continuity plan. Benchmarking, independent reviews, reporting and the development of an appropriate governance structure can provide the assurance they need to fulfill their duty.

Here are the questions that board members should ask regarding this issue:

19. **How does the board's governance structure enable it to be regularly informed of the reliability and completeness of the organization's business continuity plan, as well as of the business and financial impacts of significant incidents?**

20. **Does Internal Audit or an independent third party provide regular assurance on the effectiveness of the organization's business continuity plan and incident management process? Does management periodically benchmark its plans against best practices?**

Conclusion

The rapidly changing business, regulatory and threat environment to which most organizations are exposed requires that sustained efforts be made to ensure the ongoing availability of a reliable business continuity plan for critical business processes and services. Lack of proper attention to the development of such plans can result in major business losses, stock price declines and, at worse, the inability for the business to survive a disaster or other major disruption to its operations. The board's responsibility regarding the prevention of such losses is extensive and onerous. Clearly, all its members share responsibility for ensuring that the organization is well prepared to face emergencies. If they regularly ask the questions set out in this brochure, directors will have discharged a significant part of this duty.

Appendix — Summary of Questions

Governance Issues

1. Has the organization adopted a business continuity policy that defines management's responsibilities regarding the development, testing and maintenance of an effective business continuity plan for its critical services, business functions, systems and processes?
2. How has management ensured that formal responsibility for planning, coordinating and supporting the organization's BCP efforts is harmonized with its IT Security and Enterprise Risk Management functions?
3. Have adequate funding and resources been provided to develop and maintain the organization's business continuity plan?
4. What mechanisms have been implemented to ensure that the organization's business continuity plan complies with changes in industry practices, as well as with the laws and regulations governing the organization, both domestically and internationally?

Risk Assessment and Mitigation

5. How do business continuity plans reflect the results of the financial and operational risk assessments used to analyze the organization's exposure to various types of threats and vulnerabilities?
6. Have realistic risk scenarios been considered in the formulation of the organization's business continuity plan?
7. How does management ensure the plan is reliably updated to reflect changes to the organization's business and operational risks?
8. How does the organization ensure that its insurance coverage remains properly aligned with its evolving risk profile?

Outsourcing Issues

9. How clearly do contracts and/or service level agreements define service providers' responsibilities with respect to the organization's BCP, and enable the organization to monitor compliance?

Human Resource and Communications Issues

10. What measures has the organization taken to inform and protect its employees as well as to ensure that key expertise remains available in the event of a disaster?
11. How does executive management ensure that communications with the media and key stakeholders are duly approved and conveyed through the proper channels?
12. Are the organization's incident response plans flexible enough to enable it to respond rapidly and appropriately to various types of interruptions to its critical operations?

Change Management

13. What process has been implemented to ensure that the organization's disaster recovery plan is systematically updated and tested whenever major enhancements or routine maintenance are made to its critical information systems and infrastructures?
14. How does management ensure that plans to mitigate the risks, to its critical operations, of changes made to complex, highly integrated systems, are developed for all major projects?

Tactical Considerations

15. What alternatives to the organization's regular way of doing business have been developed to ensure the resiliency of its most critical data, systems, business functions, services and processes?
16. What steps have been taken to minimize the exposure of key personnel, and critical business and IT operations, to major crises?
17. How does management identify and protect the data and documents required to restore critical business services or functions in the event its contingency plans need to be activated?
18. Is the effectiveness of the organization's business continuity strategy regularly tested in compliance with corporate policy, or whenever significant changes alter its own technology, processes, structure, regulatory context or business environment, or those of its external service providers?

Monitoring

19. How does the board's governance structure enable it to be regularly informed of the reliability and completeness of the organization's business continuity plan, as well as of the business and financial impacts of significant incidents?
20. Does Internal Audit or an independent third party provide regular assurance on the effectiveness of the organization's business continuity plan and incident management process? Does management periodically benchmark its plans against best practices?

Notes

Notes

About the authors

The Information Technology Advisory Committee (ITAC) is part of the Knowledge Development Group at the CICA. Its role is to provide support and advice on IT matters to the CA profession and the business community.

CICA Information Technology Advisory Committee

Chair

Ray Henrickson, CA•IT, CA•CISA, Scotiabank, Toronto

Committee

Gary S. Baker, CA, Deloitte & Touche LLP, Toronto

David Chan, CA•CISA, Ontario Government, Toronto

Allan W.K. Cheung, CA•IT, CA•CISA, The Canadian Depository for Securities Limited, Toronto

Henry Grunberg, CA•IT, Ernst & Young LLP, Toronto

Carole Le Néal, CISA, CISSP, CIA, Mouvement des caisses Desjardins, Montréal

James R. Murray, CA•CISA, CA•CIA, Grant Thornton LLP, Halifax

Erlinda L. Olalia-Carin, CISA, KPMG LLP, Toronto

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•IT, CA•CISA, CISM, PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA, Office of the Auditor General of Canada, Ottawa

Gerald D. Trites, FCA, CA•IT, CA•CISA, St. Francis Xavier University, Antigonish
(also technical consultant for the Committee)

Bryan C. Walker, CA, The Canadian Institute of Chartered Accountants, Toronto

CICA Staff

Andrée Lavigne, CA, Principal, Research Studies

William J.L. Swirsky, FCA, Vice President, Knowledge Development

ISBN 1-55385-172-2

20 Questions

Directors Should Ask about the Information Technology Aspects of Business Continuity Planning

277 Wellington Street West
Toronto, ON Canada
M5V 3H2
Tel: 416-977-0748
1-800-268-3793
Fax: 416-204-3416
www.cica.ca

The Canadian Institute of Chartered Accountants