

20 Questions

Directors Should Ask about
IT

Revised April 2004



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 questions 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. Although the questions apply to most medium to large organizations, the answers will vary according to the size, complexity and sophistication of each individual organization.

The Information Technology Advisory Committee

20 Questions

Directors Should Ask about

IT

Revised April 2004

Library and Archives Canada Cataloguing in Publication

20 questions directors should ask about IT. — Rev. Apr. 2004.

(Risk management and governance collection)

ISBN 1-55385-122-6

1. Information technology — Management. 2. Management information systems. 3. Directors of corporations. I. Canadian Institute of Chartered Accountants. II. Title: Twenty questions directors should ask about IT. III. Series.

HD30.2.T88 2004

658.4'038

C2004-903966-0

Copyright © 2004

Canadian Institute of Chartered Accountants

277 Wellington Street West

Toronto, ON M5V 3H2

Printed in Canada

Disponible en français

Preface

The CICA's Information Technology Advisory Committee developed this brochure to guide the members of boards of directors in evaluating information technology 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 IT function is effective. This briefing provides suggested 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 members of the Information Technology Advisory Committee for preparing this brochure.

CICA Information Technology Advisory Committee

Chair

Donald E. Sheehy, CA•CISA, Deloitte & Touche LLP, Toronto

Committee

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

David Chan, CA•CISA, Ontario Government Information Protection Centre, Toronto

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

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

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

Carole Le Néal, CISA, Mouvement des caisses Desjardins, Montreal

James R. Murray, CA, CISA, 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•CISA, PricewaterhouseCoopers LLP, Winnipeg

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

Gerald D. Trites, FCA, CA•CISA, St-Francis Xavier University, Antigonish, NS

(also technical consultant for the Committee)

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

CICA Staff

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

Andrée Lavigne, CA, Principal, Research Studies

Board Responsibilities for Information Technology

The Board of Directors oversees an organization's overall strategic direction and management. As part of this responsibility, it must keep abreast of issues pertaining to the management and control systems in place to keep the risk of loss arising from fraud and error to an acceptable level. In addition, the Canadian Securities Administrators (CSA), in January, 2004, passed new "Investor Confidence"¹ rules that contain requirements similar to those that flowed from the *Sarbanes-Oxley Act* in the United States and establish new and important responsibilities for internal control. Of greatest interest from an IT perspective is rule 52-109, which requires the CEO and CFO to certify, among other things, that:

- they have designed disclosure controls and procedures and internal control over financial reporting (or caused them to be designed under their supervision);
- they have evaluated the effectiveness of such disclosure controls and procedures and caused their issuers to disclose their conclusions regarding their evaluation; and
- they have caused their issuers to disclose certain changes in internal control over financial reporting.

By inference, there would be a responsibility for Board members to monitor the control systems and ask the right questions to ensure that the systems are designed and operating as they should and that there are processes in place to ensure that management's legal requirements are met.

For many years, information technology (IT) has been playing an important role in the operations of organizational, strategic and managerial systems. It is often difficult, however, for generalists — which most board members are — to keep up with the rapid changes taking place in IT and, therefore, to know what questions to ask to ensure that IT issues are being properly addressed.

The TSX Guidelines on Corporate Governance, Section 474, sets out the following responsibilities of Boards of Directors:

"The board of directors of every corporation should explicitly assume responsibility for the stewardship of the corporation and, as part of the overall stewardship responsibility, should assume responsibility for the following matters:

- adoption of a strategic planning process;
- the identification of the principal risks of the corporation's business and ensuring the implementation of appropriate systems to manage these risks;
- succession planning, including appointing, training and monitoring senior management;
- a communications policy for the corporation; and
- the integrity of the corporation's internal control and management information systems."

¹ The Investor Confidence rules include Multilateral Instruments 52-108 (Auditor Oversight), 52-109 (Certification of Disclosure in Issuers' Annual and Interim filings) and 52-110 (Audit Committees).

The above list shows that an important part of a board's responsibilities is ensuring the integrity of internal control and management information systems. This responsibility is closely related to that for risk identification and evaluation, since internal control systems are generally risk based. The strategic planning process, including performance monitoring, is an important part of the control system.

This brochure suggests the questions board members should ask to carry out the responsibilities identified above. The questions that follow are grouped according to the three main areas: strategic planning, internal control and risk.



I Strategy and Planning

An important element of strategy is the strategic planning process. Strategic planning should be performed for the information systems (IS) area, and this planning must fit in with the overall corporate strategic planning exercise. This can be accomplished by having IS strategic planning integrated with the enterprise-wide strategic planning process, or as a separate exercise that is closely linked to corporate planning. IS strategic planning should encompass all of the usual elements of corporate strategic planning, including top management involvement and support, key employee involvement and the inclusion of action plans. Action plans are usually incorporated in the tactical plan. The tactical plans, developed annually, are derived from the strategic plans, but include budgets, resources, skill levels, project level information, key sponsors, etc., with periodic monitoring, update and revision.

The prime question to ask regarding strategic planning is:

- 1. Does management have a strategic information systems plan in place that is monitored and updated as required? Does this plan form the basis for the annual plans, annual and long-term budgets and the prioritization of information technology projects?**

II Technology Trends

For an organization to maintain appropriate information systems, it is important to keep up with current technology trends. This is especially important in the context of modern e-business, where there is increased integration with business partners, customers and suppliers. Organizations that retain obsolete or old systems may find it difficult to integrate them with more state-of-the-art systems, leading to lost opportunities. It is important, therefore, to track current technology trends and regularly consider upgrades of hardware and software in the context of return on investment. This effectively spreads the cost over the years, rather than having to do a massive and costly replacement of large, obsolete segments of the systems.

The question to ask here is:

- 2. Have appropriate procedures been established to ensure that the organization is aware of technology trends, periodically assessing them and taking them into consideration when determining how it can better position itself?**

III Performance

Information about organizational performance is key to any strategic planning exercise because it points to areas that can be improved or that require change to be cost-effective and efficient. Monitoring activities that can yield this information involve selection of appropriate performance metrics and development of systems to report that information to key management personnel.

Regarding organizational performance, two questions should be asked:

- 3. Have key performance indicators and drivers of the IT department been determined? Are they monitored from time to time and are they benchmarked against industry standards?**
- 4. Have relevant indicators been defined and monitored to manage the performance of the organization's third-party service providers?**

IV Personnel

The hiring and retention of appropriately skilled personnel is a challenge in the information age. Such personnel are, however, essential to the effective operation of IT systems and, to find and retain them, an organization must have strong programs in place to control the turnover, guide training, and promote professional development. It is the board that bears the ultimate oversight responsibility for the existence and effectiveness of these programs.

Two key questions here are:

- 5. How has management identified the required technology expertise and how is top talent attracted?**
- 6. Does management have appropriate procedures to address information technology employee turnover, training and project assignment?**

V Governance

There are several ways to organize the governance of IT with the actual methods, depending on factors such as the nature of the organization, its management structure, its culture and the relative importance of IT to its overall strategic objectives.

Certain principles remain relevant for most organizations. The management of IT must be directly linked to the highest executive levels of the organization. Many businesses are appointing a Chief Information Officer (CIO), who reports directly to the CEO, the audit committee and, often, the board. In some cases, the senior person responsible for IT may have other duties at the executive level that are perhaps equally or more extensive. It is generally not a good idea, however, to appoint a senior executive from finance to be in charge of IT (as has been common in the past) since that arrangement often leaves the IT function unduly focused on financial applications at the expense of other, more strategic or operational functions.

Another important principle for effective IT governance is the need to involve personnel in strategy formulation and policy implementation. This means personnel must play a meaningful role in the strategic planning process. To be effective in policy implementation, they must be aware of and subscribe to the policies. Clear communication of policies, however, is a basic and essential element of their implementation.

One of the board members should be specifically assigned to liaise with the senior IT executive and to have periodic briefings as to strategies, policies and performance.

To fulfil its IT governance mandate and to gain assurances as to compliance with Sarbanes-Oxley and the CSA Investor Confidence rules, the board should consider the following questions:

7. **Has the board considered the creation of an IT subcommittee or assigned a board member specific responsibility for the organization's investment in, and use of, information technology?**
8. **Has the responsibility for IT corporate governance been assigned to a person in a sufficiently senior management position? How does management communicate IT policies to personnel?**
9. **What procedures are in place to ensure that the company's systems and management are in compliance with Sarbanes-Oxley and/or CSA Investor Confidence rules, as appropriate?**

VI Risk and Controls

Risk and controls are related issues. In an IT context, risk relates to the probability that error or processing disruption will occur within a system that will impact the business operations of the organization. An organization must first analyze the events and circumstances that threaten its information system(s) and determine the degree of risk that exists. It is not possible, in most cases, to eliminate risk. Controls can, however, be designed, implemented and operated to reduce the risk to an acceptable level. A cost-benefit analysis is quite appropriate in this context. The acceptable level of risk establishes the type and level of controls required and, consequently, the resources to be devoted to them.

This process implies a need for a clear risk management process with regard to threats against the system, risk analysis, control implementation and monitoring. Organizations sometimes develop separate strategic security plans that must be in line with overall organizational and IT strategic plans. This is a good practice.

An essential part of any such process is an effective monitoring structure that regularly revisits the risk analyses and the adequacy of the control measures in effect. Such a monitoring structure needs to be a formal part of the organization, with reporting lines that lead to the person in charge of IT.

There are three questions to ask in the context of risk and control:

10. **Does management have a plan to periodically conduct risk assessments covering the organization's use of information technology, including internal systems and processes, outsourced services and the use of third-party communications and other services? If it does, are the results of the assessments acted on where appropriate or required?**
11. **How does management ensure data integrity, including relevance, completeness, accuracy and timeliness, and its appropriate use within the organization?**
12. **What arrangements does the organization have for the regular review and audit of its systems to ensure risks are sufficiently mitigated and controls are in place to support the major processes of the business?**

VII Personal Information Privacy

Information privacy is a priority of business that requires constant attention. The passage of new federal and provincial privacy legislation has established new and often strict rules with regard to data ownership and the steps that organizations in possession of private information must take to protect individuals' privacy. This legislation, as well as similar legislation elsewhere in the world, is contributing to a new environment regarding information privacy, where corporations must assume greater responsibilities.

Because of these new responsibilities, many organizations have established policies specifically to deal with privacy. Some have appointed privacy officers to develop and communicate policies on privacy issues and legislative requirements, to monitor those policies and to act as a resource for organizational personnel on privacy matters. In addition, of course, these officers serve as important members of the management team to ensure that privacy matters are considered in the development of new initiatives.

Here, the questions to ask are:

- 13. Has the organization assigned someone the responsibility for privacy policy, privacy legislation and compliance therewith?**
- 14. Has the organization identified the various legislative and regulatory requirements for protecting personal information and developed a policy and procedures for monitoring compliance with them?**

VIII E-business

The entry of an organization into e-business activities not only introduces new IT risks, it can also increase the risks that already existed. This greater risk derives from the fact that e-business relies upon the Internet and, as such, suffers from all the threats that abound there.

The threat of intrusion via the Internet, or through a widely dispersed private network, requires enhanced controls. These control measures could include the installation of firewalls, intrusion detection systems, enhanced user identification and password systems and the formulation of related policies that raise access control to a level commensurate with this considerable risk. The level of risk in the particular circumstances needs to be fully reviewed and evaluated. Risk is influenced by the nature of the business, its profile, the kind of customers it attracts and the methods of payment in use.

Two pertinent questions to ask are:

15. **If the organization uses e-business to buy or sell products or services, has there been a specific review of the risks and controls over the e-business activities?**
16. **Are the organization's e-business activities appropriately protected from external and internal attack by unauthorized persons or others that, if successful, would result in loss of customer satisfaction or public embarrassment?**

IX Availability

Most businesses are now hugely dependent on their information systems and, when those systems go down, experience lower productivity because some or all personnel are unable to do their jobs. It is paramount that plans be in place to ensure that systems will be brought back into production and made fully operational as soon as possible following a service outage. Availability requires the development of formal recovery plans that are tested and maintained in a ready state at all times.

As with any control issues, the degree of risk is relevant to the extent of control employed. A centralized system, for example, is normally exposed to greater risk than one that is dispersed because, with the latter, there is a greater opportunity to spread the risk within the system. Even in these situations, however, some planning is necessary to be able to use the capacity in other parts of the system to compensate for the part that is down. One of the factors to consider in evaluating the degree of risk is the extent to which the organization has experienced downtime.

In this context, the board needs to ask:

- 17. Has the organization adopted formal availability policies? Has it implemented effective controls to provide reasonable assurance that systems and data are available in conformity with availability policies?**
- 18. Does the organization understand the impact of an interruption in service and are there plans in place to deal with potential interruptions? Has a business continuity plan been adopted? If it has been adopted, is it tested regularly and are the results used to improve the plan?**

X Legal Issues

Some legal issues have arisen with regard to compliance with software licences, particularly as a result of illegal copying of software and using copied software in organizational systems. Intellectual property has increasingly been an issue in litigation, and some organizations have ended up paying extremely heavy fines. The board bears ultimate responsibility when such matters have a significant impact on an organization.

Management should implement specific programs that will minimize the risk of violating the law in this area. An important element of management's approach is the "tone at the top." It is essential that management impresses on its personnel that the use of unauthorized or illegally copied software or data and related legal violations is not acceptable. Many firms also take precautions such as annual software audits, prescribed procurement policies and periodic review of legal agreements to establish that procedures are in place to deal with all legal obligations. These issues can also be addressed by instituting policies to ensure that the information systems are used for acceptable business purposes.

The questions to ask:

- 19. Has management considered and addressed legal implications that pertain to the use of software, hardware, service agreements and copyright laws?**
- 20. Have policies covering licences, agreements, copyright and acceptable use been formulated and disseminated to all personnel?**

Follow Up on Replies

The board may delegate some of these issues, along with the questions to ask, to the audit committee. The extent to which this is done will, of course, vary from one organization to another. The board can discharge its responsibilities regarding any issues being dealt with by the audit committee simply by making inquiries of the audit committee and discussing the responses.

It is essential to have a follow-up program of the responses. If questions are asked and the answers indicate that procedures will be implemented to deal with perceived shortcomings in the control system, the board must follow up at the next meeting to determine whether, in fact, those procedures have been implemented. If the audit committee is looking after that particular area, the board's role may be simply to determine that the committee has a follow-up procedure in place and has no further issues to report. If the audit committee is not involved in this area, board members must make follow-up inquiries of management at the earliest opportunity. Depending on the results, further specific follow-up steps may be appropriate.

Conclusion

For many organizations, information technology has become such a pervasive and complex part of operations that a breakdown in IT systems can bring them virtually to a standstill. As a result, lack of attention to proper control over the systems can be expensive indeed, sometimes causing major business losses, stock price declines and consequent loss of market capitalization. In these situations, the extent of the board's responsibility is apparent and onerous.

Clearly, all board members must take responsibility for paying close attention to the issues raised by information systems. If they regularly ask the questions outlined in this brochure, they will have discharged a significant part of those duties.

Appendix — Summary of Questions

Strategic Issues

I Strategy and Planning

1. Does management have a strategic information systems plan in place that is monitored and updated as required? Does this plan form the basis for the annual plans, annual and long-term budgets and the prioritization of information technology projects?

II Technology Trends

2. Have appropriate procedures been established to ensure that the organization is aware of technology trends, periodically assessing them and taking them into consideration when determining how it can better position itself?

III Performance

3. Have key performance indicators and drivers of the IT department been determined? Are they monitored from time to time and are they benchmarked against industry standards?
4. Have relevant indicators been defined and monitored to manage the performance of the organization's third-party service providers?

IV Personnel

5. How has management identified the required technology expertise and how is top talent attracted?
6. Does management have appropriate procedures to address information technology employee turnover, training and project assignment?

Internal Control Issues

V Governance

7. Has the board considered the creation of an IT subcommittee or assigned a board member specific responsibility for the organization's investment in, and use of, information technology?
8. Has the responsibility for IT corporate governance been assigned to a person in a sufficiently senior management position? How does management communicate their IT policies to personnel?
9. What procedures are in place to ensure that the company's systems and management are in compliance with Sarbanes-Oxley and/or CSA Investor Confidence rules, as appropriate?

Risk Issues

VI Risk and Controls

10. Does management have a plan to periodically conduct risk assessments covering the organization's use of information technology, including internal systems and processes, outsourced services and the use of third-party communications and other services? If it does, are the results of the assessments acted on where appropriate or required?
11. How does management ensure data integrity, including relevance, completeness, accuracy and timeliness, and its appropriate use within the organization?

12. What arrangements does the organization have for the regular review and audit of its systems to ensure risks are sufficiently mitigated and controls are in place to support the major processes of the business?

VII Personal Information Privacy

13. Has the organization assigned someone the responsibility for privacy policy, privacy legislation and compliance therewith?
14. Has the organization identified the various legislative and regulatory requirements for protecting personal information and developed a policy and procedures for monitoring compliance with them?

VIII E-business

15. If the organization uses e-business to buy or sell products or services, has there been a specific review of the risks and controls over the e-business activities?
16. Are the organization's e-business activities appropriately protected from external and internal attack by unauthorized persons or others that, if successful, would result in loss of customer satisfaction or public embarrassment?

IX Availability

17. Has the organization adopted formal availability policies? Has it implemented effective controls to provide reasonable assurance that systems and data are available in conformity with availability policies?
18. Does the organization understand the impact of an interruption in service and are there plans in place to deal with potential interruptions? Has a business continuity plan been adopted? If it has been adopted, is it tested regularly and are the results used to improve the plan?

X Legal Issues

19. Has management considered and addressed legal implications that pertain to the use of software, hardware, service agreements and copyright laws?
20. Have policies covering licences, agreements, copyright and acceptable use been formulated and disseminated to all personnel?

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

Donald E. Sheehy, CA•CISA, Deloitte & Touche LLP, Toronto

Committee

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

David Chan, CA•CISA, Ontario Government Information Protection Centre, Toronto

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

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

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

Carole Le Néal, CISA, Mouvement des caisses Desjardins, Montreal

James R. Murray, CA, CISA, 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•CISA, PricewaterhouseCoopers LLP, Winnipeg

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

Gerald D. Trites, FCA, CA•CISA, St-Francis Xavier University, Antigonish, NS

(also technical consultant for the Committee)

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

CICA Staff

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

Andrée Lavigne, CA, Principal, Research Studies

ISBN 1-55385-122-6



9 781553 851226

20 Questions

Directors Should Ask about

IT

Revised April 2004

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