Chartered Accountants of Canada

20 Questions Directors Should Ask about IT

Second edition

WRITTEN BY
Gary S. Baker, BBA, CA, CGEIT

20 QUESTIONS

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 provide directors with a basis for critically assessing the answers they get and digging deeper as necessary.

The comments summarize current thinking on the issues and the practices of leading organizations. 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.

WRITTEN BY
Gary S. Baker, BBA, CA, CGEIT

PROJECT DIRECTION
Gigi Dawe
Principal, Risk Oversight and Governance
CICA

Cecilia Banh, CA, MAcc
Principal, Guidance and Support
CICA

INSTITUTE OF CORPORATE DIRECTORS

The CICA has granted permission to the ICD to use these materials in its Director Education Program.

Chartered Accountants of Canada

20 Questions Directors Should Ask about **IT**

Second Edition

Library and Archives Canada Cataloguing in Publication

Baker, Gary, date

20 questions directors should ask about IT [electronic resource] / Gary Baker. -- 2nd ed.
Electronic monograph in PDF format.
Issued also in print format.

ISBN 978-1-55385-725-9

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

HD30.2.B338 2012 658.4'038 C2012-906530-7

Preface

To help board members fulfill their responsibility for the oversight of an organization's business activities, the Information Management and Technology Advisory Committee (IMTAC) and the Risk Oversight and Governance Board (ROGB) of the Canadian Institute of Chartered Accountants (CICA) have commissioned this re-issue of its publication '20 Questions Directors Should Ask about IT'. This second edition has been updated to reflect changes in the business and information technology environments since the first edition was published.

The directors' oversight role includes assuring themselves that objectives are achieved, risks are managed appropriately and the organization's resources are used responsibly. As information and its supporting technology become increasingly important to the success of an organization, governance of the organization's use and management of its information and information resources, systems and technology is becoming an increasingly critical and necessary component of board activities. This briefing provides suggested questions for directors to ask the CEO, senior management, professional advisors — and themselves. Directors and CEOs will find it useful in assessing their present approach to overseeing the use of information assets throughout organizations for which they are responsible. Reading this document may also prompt dialogue among directors and between boards and executives. That's exactly what effective governance is all about.

IMTAC and the ROGB thank the author, Gary Baker, and acknowledge the contribution of the Directors Advisory Group. They identified the need for research and guidance in this important area and have provided high-level commentary and suggestions to the author throughout the course of his work.

Mario Durigon, CA
Chair, Information Management and Technology Advisory Committee

Huw Thomas, CA
Chair, Risk Oversight and Governance Board

Contents

Executive Summary – Why Directors Should Ask Questions about IT[1]

Because computerized information systems are an essential element in today's business environment, they are a necessary element of board members' oversight responsibilities. While IT often appears to deal with matters that can be quite technical, it is important that board members are not overwhelmed by the technical details. First and foremost the issues must be considered in the context of their business impact and not as technical issues. Board members need to provide oversight and governance related to the business implications of information technology.

All companies are faced with significant information-technology-related issues and opportunities that need board members to be asking the right questions to help their companies make the right decisions. Taking advantage of opportunities at the right time can provide an organization with significant competitive advantage; lack of board oversight and not asking the right questions, can put the organization at significant risk.

Common business issues being faced by companies and their boards include[2]:

- **Leveraging emerging technologies** – Technological innovations can present significant business opportunities for those organizations that capitalize on them at the right time and sustain that advantage. There can be significant cost (financial, social and HR) to being on the "bleeding edge" of technology. On the other hand, it may be difficult to recover from missed opportunities. Boards have a significant role in challenging business strategies and providing appropriate direction to management to be satisfied the organization is adopting and maintaining relevant technology that achieves and sustains competitive advantage and business value.
- **Major systems implementation, conversion or outsourcing initiatives** – Business literature is filled with horror stories of systems implementations and outsourcing projects gone wrong that have cost the organization tens or even hundreds of millions of dollars. These project failures can cause significant reputational or financial damage and operational disruptions. Major systems projects can have a major impact on the success of the organization. Boards need to be satisfied that:
  - Ownership and accountability rests with appropriate senior business management,
  - Responsibility has been appropriately assigned for defining business and functional requirements,
  - Appropriate processes and controls are in place to acquire, deploy and operate these solutions,
  - The organization has the capacity to properly manage and successfully complete these business transformations,
  - Executive management, and where appropriate the board, is receiving timely, accurate and faithful reporting and providing an appropriate level of oversight.
- **Privacy and other information security exposures** – Organizations don't want and certainly don't need the public embarrassment and other consequences that come with being victims of hacker attacks, breaches of privacy legislation or industrial espionage. Boards need to be asking the right questions to be satisfied their companies have appropriate risk management practices and protection measures in place to mitigate these security exposures.
- **Business recovery and continuity** – Dependence on electronic information

1 IT is an acronym often used to refer to a variety of things, and can mean different things to different people. For the sake of clarity, throughout the rest of this document we will use the following terminology and definitions:
- information and information resources, systems and technology - as the broader definition of the domain addressed in this document. It is intended to include the organization's information, regardless of form or media, and the people, processes, hardware and software involved in generating and using that information.
- information assets - for convenience, as a shorter form of "information and information resources, systems and technology".
- IT - to refer to the functional group of people or department within the organization typically assigned primary responsibility for managing the computer hardware, software and data (except when used in nouns, titles, quotes or reference to those quotes).

2 Additional information on technology trends and issues can be obtained from the September issues of CAMagazine where the CICA publishes current trends in technology and their business impact.

means it can be difficult or impossible to conduct business if the information and corresponding information systems are not available when needed. This is not simply an IT disaster recovery issue. This is a business issue that requires collaboration between the business and IT to understand the business requirements and ensure that both IT and business plans are in place to ensure the organization is prepared to deal effectively with unforeseen events. The board plays a critical role in asking the right questions to make sure appropriate plans are in place and will work when required.

- **Size of capital expenditures and operating costs related to IT** – Information technology is a significant capital expenditure for many organizations. Organizations may not have meaningful insights into the true costs of their systems and the value they deliver. This points to the need for board oversight to make sure that capital expenditures are appropriate and consistent with the strategic and business objectives of the organization, and that the costs – project costs as well as operating costs – are appropriate and provide value to the organization.
- **Legal, regulatory, and operational compliance issues** – Many organizations are faced with a rapidly growing list of legal, regulatory, and operational compliance matters related to its information and information assets including integrity of financial reporting, privacy legislation, patent and trademark infringement, and industry-specific legislative requirements. Boards need to be satisfied that management has taken appropriate measures to identify, manage and satisfy these compliance requirements.

All too often board members are in a position of having to react after things have gone wrong. They find themselves reflecting on "what questions should we have asked that might have prevented this situation." The purpose of this document is to assist board members with the kinds of questions they need to be asking (questions that may not be on their list at the moment but should be) to satisfy their governance responsibilities, and ensure management is taking appropriate steps to prevent these issues from occurring in the first place.

However, governance is not a "one-size-fits-all" activity and the same is true for the governance of information assets. The kinds of questions board members need to be asking depend very much on the organization, its use of information technology, and the competitive environment in which it operates. This document has been organized to assist board members in asking the right questions. The questions in this document are organized around three key issues that boards need to address:

Key Issue	Relevant Section
The role the board should have with respect to governance of the organization's information assets	**Part A** – The Role of the Board in Governing Information Assets
The appropriateness of the organization's information asset strategy to capitalize on opportunities and maximize the value of its information assets	**Part B** – Information-Asset Strategy and Its Value to the Organization
The ability of the organization to effectively manage performance and risks related to its information assets	**Part C** – Governing Information Asset Management and Performance **Part D** – Governing the Organization's Information Asset Risks

Finally, **Part E – The Board's Use of Information and Information Systems** – This Part provides an opportunity for boards to reflect on their own use of information and information technology to improve the efficiency and effectiveness of board activities.

> The question is no longer whether the board should be involved in IT decisions; the question is, how?
>
> Richard Nolan and F. Warren McFarlan

Part A – The Role of the Board in Governing Information Assets

Questions in this section deal with the board understanding and defining its role with respect to governance matters related to information and information resources, systems and technology. These questions also ensure the board has the appropriate resources and is provided with appropriate, timely information to satisfy that role. These questions are important for all organizations. While the specific role of the board will vary from organization to organization, it is important that board members give proper consideration to what their role should be and how they will satisfy it.

Key questions include:

1. What is the strategic importance of its information assets to the organization?
2. What role should the board have in governing information assets?
3. How does the board ensure it has the right skills, knowledge and competencies to effectively discharge its role?
4. How and when are matters related to the organization's information assets reported to the board?

1. What is the strategic importance of its information assets to the organization?

Not all organizations use information and information resources, systems and technology (collectively referred as 'information assets') in the same way, nor are they at the same point in their adoption and use. It is important that an organization and its board understand the scope and role that its information assets have in the organization's success, so the organization can adopt appropriate strategies, governance and management processes.

A variety of frameworks and models have been published that boards and organizations may find useful to structure and clarify their thinking around the strategic importance of the organization's information assets. Such frameworks and models suggest a range of postures that organizations can adopt toward information and information technology, from maintaining the status quo to leveraging information technology as a means of competitive differentiation. These models can provide a useful tool to help position the strategic importance of information assets for an organization.

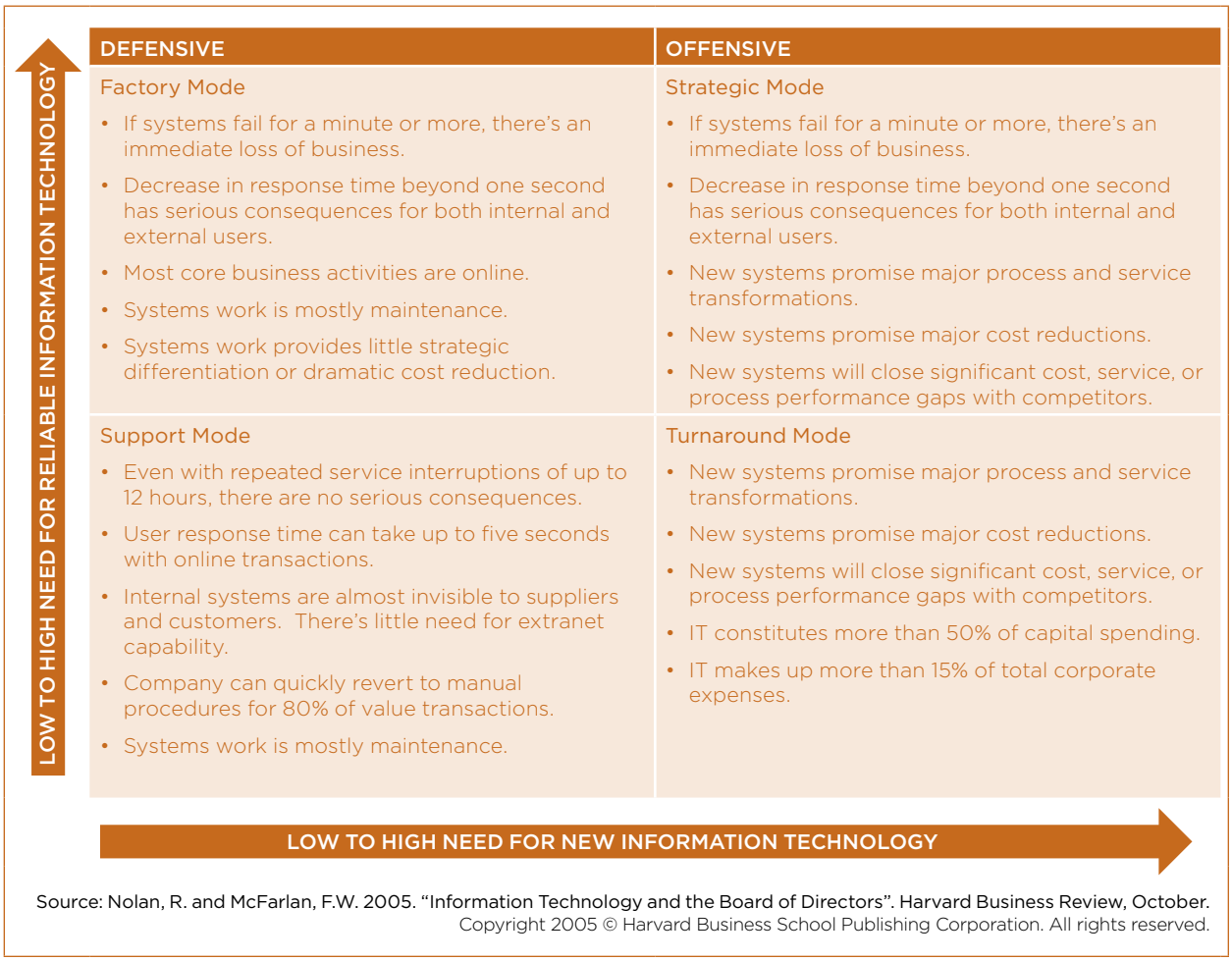
One such model, The "IT Strategic Impact Grid" (see Exhibit 1) developed by Richard Nolan and F. Warren McFarlan of Harvard Business School (Nolan and McFarlan), defines the importance and value of information assets to an organization based on two concepts. Firstly, the extent to which a company relies on smoothly operating, cost-effective, information systems. Secondly, the extent to which the company relies on IT as a part of its competitive advantage for new business models, products and services or enhanced customer responsiveness.

Organizations operating on the Defensive side of the continuum are typically focused on **operational reliability**. Information technology tends to be more of a utility function and the information asset strategy is focused on providing reliable, cost-effective information to achieve the organization's existing business strategy, goals and objectives. Organizations in *Support Mode* have less reliance on information assets and the impact associated with a lower degree of reliability of their systems is less significant. In *Factory Mode* organizations are more dependent on their information assets and are more severely impacted by their reliability.

While the focus for these organizations may be more operational and less strategic, it is necessary to monitor emerging threats and opportunities to remain competitive and maintain marketplace positioning.

For organizations operating on the Offensive side of the continuum, the focus moves towards the strategic use of information assets for capitalizing on new and emerging business opportunities. Information assets and business strategies are more intertwined and need to be closely aligned to enable the organization's success. In *Turnaround Mode,* organizations are looking at strategic investments in information assets to improve their competitive position by, for example, reducing costs and closing performance gaps with competi-

Exhibit 1 — IT Strategic Impact Grid



Source: Nolan, R. and McFarlan, F.W. 2005. "Information Technology and the Board of Directors". Harvard Business Review, October.

tors. Organizations in *Strategic Mode* require high reliability and use their information assets as strategic assets to innovate and transform business models by, for example, developing new products and services to gain and maintain significant competitive advantage in the marketplace. In both *Turnaround* and *Strategic Mode*, investments are often significant, both in terms of capital requirements and the degree of organizational change.

In asking about the strategic importance of its information assets to the organization, the board should understand where the organization is currently positioned (on the "IT Strategic Impact Grid", for example). This questioning will assist the board to determine whether the organization's strategy for information assets is appropriate given their strategic importance and value to the organization. It can also enable the board to ensure that the organization's information asset strategy, goals and objectives are aligned with the organization's overall business strategy, goals and objectives. For example, if an organization's business strategy is to hold a dominant position in its market, it may require a more Offensive information asset strategy (i.e., more closely aligned with the *Turnaround Mode* and *Strategic Mode*) as opposed to a Defensive information asset strategy (such as in *Factory Mode* and *Support Mode*), which is unlikely to enable the organization to achieve or hold a dominant position.

In addition to understanding the organization's current position, it is important that the board consider where the organization *should* be positioned. The board needs to consider whether

the organization's current position is appropriate, or whether it needs to adopt an information asset strategy to re-position the value and importance of its information assets to achieve its business strategies, goals and objectives. For example, if an organization is facing competitive pressures and needs to improve its competitive positioning, the organization may require an information asset strategy that will enable it to move closer to *Turnaround Mode*. Maintaining a *Factory Mode* or *Support Mode* of operations is unlikely to enable the organization to improve its competitive positioning.

The strategic importance of information assets will vary among organizations, and likely vary among business units within the same organization. Understanding the strategic importance of its information assets is important to enable the board to evaluate strategic alternatives, provide direction to management and to monitor organizational performance.

2. What role should the board have in governing information assets?

Board members serve as representatives of the organization's shareholders to provide oversight and direction to management in the affairs of the organization. The board's role is to evaluate strategic alternatives, provide direction to management and to monitor management and organizational performance on behalf of the shareholders. As noted by the IT Governance Institute in its definition of IT governance (see below), the enterprise's governance of its information assets is an integral component of enterprise governance overall.

> "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."
>
> IT Governance Institute

In satisfying its corporate governance role, the board needs to consider what role it needs to have for the governance of the organization's information assets. Governance is not a "one-size-fits-all" undertaking. The strategic importance and value of its information assets vary among organizations and as such, the role and governance activities of the board should also vary.

It is important for the board to adopt an appropriate role for governing the organization's information assets based on the strategic importance and value of those assets to the organization. This role and associated responsibilities should be incorporated into the board's mandate.

For organizations operating in *Support Mode* or *Factory Mode* it may be more appropriate for the board to focus its oversight on matters such as operational performance and management of the information assets as well as management of the risks associated with them. For these organizations it may be appropriate for the board to place more emphasis on the questions pertaining to performance management and risk management (Parts C and D).

For organizations operating in the *Turnaround Mode* or *Strategic Mode*, issues related to operational performance and the management of related risks continue to be important for the board to consider. However, the board also needs to place emphasis on questions relating to the importance and value of the information assets to the organization and its corporate strategy (Part B).

In both situations, it is important that the organization's overall strategy appropriately includes the organization's information assets. Particularly for *Turnaround Mode* or *Strategic Mode* companies, strategies for information and information resources, systems and technology are an integral component of the overall corporate strategy. The board needs to ensure the organization's business and information asset strategies are aligned and integrated and that sufficient, appropriate resources are allocated to enable achievement of those strategies.

While maintaining its overall responsibility, the board may choose to delegate other components of governance of information assets to various committees or equivalents.

Audit and Finance Committee(s)

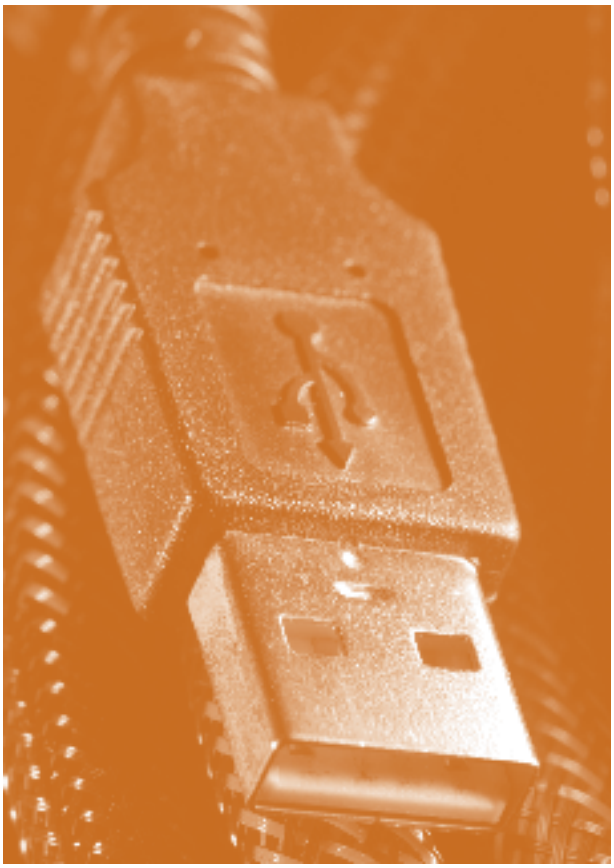
In many organizations the audit and finance committee(s) plays a key role in providing oversight of the financial management of the organization and the management of the organization's business risks. With respect to the governance of information assets, particularly for organizations in *Support Mode* or *Factory Mode*, the audit and finance committee(s) may be appropriate to oversee matters related to:

- Establishment and monitoring achievement of information-asset-related operational goals and objectives
- Approval and successful execution of technology-enabled business initiatives
- Management of information-asset-related risks such as integrity, reliability, confidentiality and availability.

Risk Management and Governance Committee

Where boards have established a committee for these matters separate from the audit and finance committee(s), the committee's responsibility should extend to include the governance, risk management and compliance activities related to the organization's information assets. Particularly important for organizations in *Factory Mode* or *Turnaround Mode*, this could include oversight of such activities as:

- Adoption and implementation of an IT management frameworks such as COBIT and ITIL[3]
- Inventorying and classification of information assets
- Identification, assessment and monitoring of business risks related to information assets, as part of the organization's risk and compliance management processes
- Completion of regular security and compliance audits.



IT Oversight Committee

Creating a board-level IT committee devoted to the oversight of an organization's information assets is not a practice all companies should necessarily adopt. For example, some firms such as consulting firms, small retailers, and small manufacturers may not have the time and resources to set up a separate IT committee. In some cases however, particularly for *Strategic Mode* organizations, it may be appropriate to establish a separate committee responsible for oversight of the organization's information assets. Such a committee would be responsible for monitoring emerging trends and identifying and assessing competitive threats and opportunities. This committee should be challenging the CEO and the CIO of the organization about the business implications of emerging technologies and new business models, products and services emerging in the marketplace.

Whether the board delegates oversight responsibilities to various committees, or chooses to retain the oversight role, the board has ultimate respon-

3 COBIT is a framework created by ISACA for information technology (IT) management and IT Governance. The purpose of COBIT is to provide management and business process owners with an IT governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. See Appendix 2 for additional information related to COBIT.
The Information Technology Infrastructure Library (ITIL), is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

sibility. As such, the board should be proactive and not simply reactive to crisis situations created by competitor initiatives, security incidents, project or system failures, or audit findings.

Appendix 1 provides a sample Board IT Governance Calendar for the kinds of activities boards should consider incorporating as part of their calendar of activities (either at the board level or within the appropriate committees of the board).

3. How does the board ensure it has the right skills, knowledge and competencies to effectively discharge its role?

To satisfy its role in the governance of information assets, it is necessary for the board to ensure that it has the appropriate information-technology-related skills, knowledge and competencies within its membership. Board-level discussions about information assets can be challenging. The board needs to ensure such discussions stay focused on the business issues and opportunities, and not get bogged down in technical minutia and detail. Some of the related skills and competencies the board should consider include:

Technical and management expertise

Depending on the strategic value and importance of information assets to the organization and the role of the board, it is important for some board members to have basic knowledge and understanding of the existing and emerging technologies relevant to the organization. It is also desirable that some board members have knowledge and understanding of the business implications of the acquisition, deployment and operation of information systems. For organizations where its information assets have a higher strategic value and importance, both the proportion of board members with related skills and the depth of those competencies should correspondingly increase. One of the roles of these board members is to challenge conventional thinking and provoke innovation.

Knowledge of the organization's information assets, competencies and capabilities

The board needs to develop and maintain an appropriate knowledge and awareness of the organization's information assets. Knowledge of these assets will, in turn, enable the board to develop an understanding of the organization's information-related capabilities. This knowledge and awareness is essential to enable the board to effectively evaluate alternatives, provide direction and monitor organizational performance related to the organization's information assets.

Knowledge of the industry and competitor use of IT

In addition to having an understanding of the organization's information assets, it is important for the board to have an appropriate level of knowledge of the importance and use of information and related technologies within the industry and by its competitors. Having this understanding is necessary for the board to have a meaningful context for fulfilling its oversight responsibilities.

Knowledge of emerging IT trends and capabilities

It is also important that at least some board members are aware of emerging trends and the business implications of these trends. Current trends such as cloud computing[4], social networking[5], the adoption of smartphones and the corresponding increase in mobile computing represent disruptive technologies that provide significant opportunities or significant competitive threats. Awareness of these trends and their corresponding business implications requires the board to be more proactive in its oversight role rather than having to react in potential crisis situations.

Knowledge of the organization's key information-asset-related business risks

To enable it to provide appropriate oversight of the organization's risk management policies and prac-

4 **Cloud Computing** refers to the provision of computing capability by way of a service. Organizations can, for example, acquire computing capability through purchasing these services (typically as a "pay-per-use" or operating cost) from a supplier as an alternative to investing in capital assets by acquiring and implementing the computer hardware and software. For additional information see ITAC Brief – *Cloud Computing: A Primer*, published by the CICA.

5 **Social Networking** or **Social Media** refers to the use of Internet and mobile based technologies to enable interactive communication among individuals, organizations or communities of interest. For information on governance issues relating to adopting a social media plan, refer to the January 2012 Director Alert Published by the CICA's Risk Oversight and Governance Board. In addition, further information can be found in the March 2012 joint publication by the CICA's Canadian Performance Reporting Board (CPRB) and the Canadian Investor Relations Institute (CIRI) titled Role of *Social Media in Performance Reporting – A Discussion Brief*.

tices, the board needs to have an understanding of the key business risks related to the organization's information assets.

The importance in having knowledge of the organization's information assets and their corresponding business implications is no different than for other knowledge domains of the board such as finance and executive compensation. There are challenges placed on boards to obtain, maintain and effectively utilize related knowledge under time and resource constraints. In addition, the board needs to balance these demands with other priorities they may have. As information assets become an increasingly important contributor to the organization's success, finding solutions to these challenges also becomes increasingly important. Some techniques boards should consider include:

- **Recruiting board members with skills and experience in information and information resources, systems and technology** – Such attributes should be included in the candidate evaluation and selection process. As board members, such individuals need to be able to translate the technical jargon and effectively communicate issues in business terms.
- **Engaging an external advisory group/ sounding board** – This group would advise and assist board members on matters related to information and information resources, systems and technology and its business implications.
- **Periodic training and awareness sessions** – These sessions would be part of the board's regular education and development activities. They could include presentations on such topics as emerging technologies; awareness of organizational information assets and capabilities; and related business risks, exposures and vulnerabilities.
- **Maintaining information-and-technology-related competencies as part of board members' skills matrix, and conducting periodic board member skills and competency reviews** – These competencies and skills would be reviewed either through self-assessment or by an independent external advisor. The skills matrix and periodic assessment will provide an objective view of the competencies represented on the board compared with the competencies that may be required or desired.

4. How and when are matters related to the organization's information assets reported to the board?

In order for the board to effectively fulfil its role, it is essential that it be provided with sufficient, appropriate and timely information on relevant matters relating to information assets. Two of the most common triggers for including such matters on the board's agenda have historically been:

- when approval is needed for funding significant technology-related investments and capital expenditures; and
- in reaction to a technology-related problem or incident.

While these are important triggers, they fail to provide the board with timely, sufficient and appropriate information that would enable the board to properly fulfil its role. Depending on the strategic importance of the organization's information assets and the board's role with respect to governance of these assets, boards need to be proactive in defining the nature, extent, timing and frequency of reporting of information assets and the board's expectations of management. In addition to funding requests and explanations of problems, boards should establish reporting requirements related to:

- information-asset strategy and value, performance and management of information assets and their related business risks. Questions in the remaining sections are designed to assist board members identify their requirements in these areas;
- management reports provided by individuals from within the organization such as the chief executive officer, chief information officer, chief audit executive, corporate risk management and compliance, chief privacy officer, and the chief information security officer.

Part B – Information-Asset Strategy and Its Value to the Organization

Questions in this section relate to the board's role in evaluating, directing and monitoring the organization's strategies, goals and objectives. The board needs to understand the strategic importance of the organization's information assets, whether that level of strategic value and importance is appropriate given the environment and business goals of the organization, and whether it continues to be appropriate over time. These questions are particularly relevant for organizations dealing with the alignment of information-asset strategies with overall organizational strategies, and with the monitoring of trends and the assessment of their impact on the business. Their relative importance varies with the overall strategic importance that information assets have to the organization.

Key questions include:

5. How does management ensure the organization's information-asset strategy is aligned with the organization's overall strategy, and is appropriate given the strategic importance of its information assets?
6. What role does the management team have in developing and implementing the organization's information-asset strategy?
7. Do the organization's information assets give the organization the agility required to capitalize on, and adapt to marketplace forces and opportunities?
8. Do the board and management know and understand the value of the organization's information assets?
9. How are the value and contribution provided by the organization's information assets defined and measured?
10. How are emerging technologies and trends, and their potential impact on the organization monitored and assessed?

5. How does management ensure the organization's information-asset strategy is aligned with the organization's overall strategy, and is appropriate given the strategic importance of its information assets?

A key objective of information assets in most organizations is to facilitate the capturing and processing of information to ensure achievement of business goals and objectives. Many organizations are also experiencing the convergence of their information systems with other technologies such as engineering systems, process automation systems and shop-floor control systems. To maximize the value achieved, it is essential there be a close alignment of the organization's information-asset strategy with the overall corporate strategy.

In addition to being aligned with the organization's overall corporate strategy, the information-asset strategy needs to reflect appropriate direction, activities and investment priorities. For an organization operating in *Support Mode* or *Factory Mode*, the information-asset strategy might be principally focused on providing data processing service that is complete, accurate and timely to meet business requirements. While an organization in *Support Mode* may be principally focused on efficiency and cost-effectiveness, an organization operating in *Factory Mode* could place increased emphasis on accuracy, reliability and availability of its information assets and processing capability.

Organizations operating in *Turnaround Mode* or *Strategic Mode* are likely to require more aggressive, far-reaching information-asset strategies that include capitalizing on new and emerging technologies. In *Turnaround Mode*, information-asset strategies will need to focus on enabling business process transformations, improving competitive positioning and enabling significant cost reductions and/or performance improvements. For organizations in *Strategic Mode*, information-asset strategies will also need to focus on product and service innovations, enabling new operating and business models, and enhancing information-asset security, integrity, reliability and availability.

Boards should also understand the organization's philosophy and, accordingly, be able to provide appropriate strategic direction with respect to its information assets. For example, is the organiza-

tional philosophy to build custom applications or to buy commercially available solutions (make vs. buy)? Is the approach one of developing internal capabilities or leveraging external service providers (in-source vs. outsource or buy vs. rent)? Is the operating model a centralized information processing facility or is processing distributed to the business unit level (centralized vs. decentralized)? It is not a question of whether one of these philosophies is better or worse than another, but rather whether the philosophy and strategic direction is commonly understood and meets the business requirements of the organization.

6. What role does the management team have in developing and implementing the organization's information-asset strategy?

Organizational use of information assets has evolved dramatically from simply being a tool to record business transactions or other non-financial events (as characterized by the term "electronic data processing") to being an enabler of business models, products and services and business solutions. Examples of just a few of the ways in which organizations are leveraging their information assets include:

- enabling new business models such as selling direct to customers – bypassing wholesalers and distributors (some examples are digital entertainment and media distribution, online retail storefronts, and real-time news distribution);
- enabling trading-partner and customer collaboration on product design, engineering, manufacturing and service;
- enabling innovative business solutions such as access to global markets and customer self-service from order processing to training, troubleshooting and problem resolution;
- facilitating communications with stakeholders, business partners and customers through websites, audio and video webcasts, CEO blogs, and interactive customer chat sessions.

The growing significance of information assets and the impact they have (and will have) on the overall business require all areas of management to understand the power of these assets to change the business. Management must understand how it will play a role in leveraging information assets to develop and implement the organization's strategies, goals and objectives. It is no longer appropriate to just "delegate IT" to the CIO. Information assets are such an important element in all aspects of the business that management needs to accept ownership, responsibility and accountability for them.

Some of the attributes, characteristics and areas where boards should be challenging management include:

- Management's awareness and understanding of the capability of information assets to impact, disrupt, and/or fundamentally change the business.
- The CIO's ability to help identify, interpret and exploit the business implications of information assets. The CIO plays an important role as an intermediary or "translator" between the technologists and business management. The CIO needs to be actively engaged as a member of the management team and be effective in communicating in business language the implications, threats and opportunities associated with information assets.
- The responsibility and accountability of each member of the management team for leveraging the organization's information assets in developing and implementing business strategies, goals and objectives.

7. Do the organization's information assets give the organization the agility required to capitalize on, and adapt to marketplace forces and opportunities?

Today's business marketplace is a dynamic, rapidly changing environment. To remain competitive, organizations need to anticipate marketplace changes and adapt to them quickly. Market leaders maintain their leadership positions by being able to anticipate and capitalize on marketplace changes through innovative solutions. Information assets are one of the major levers organizations have used to adapt to marketplace changes.

For example, current technological innovations such as smartphones, tablets, social networking and wireless networking are having a significant impact on the delivery of goods and services to consumers and the nature of the relationship between organizations and their customers. These innovations are providing consumers with increasing expectations for immediate gratification, easier access to competitive products and services, and opportunities to share their experiences with

others. The board needs to challenge management on whether the organization's information assets provide the agility needed to capitalize on the opportunities and the discipline to manage the threats posed by such innovations. Is the organization able to leverage its information assets and the capabilities of its business partners (such as cloud computing service providers) to minimize the lead time necessary to adapt its products and services? Also, does the organization have appropriate strategies, policies and procedures in place to ensure it is utilizing these innovations (such as social networking) to strengthen relationships with its customers and to monitor what the marketplace is saying?

Ultimately, the organization's business capability can be limited by what its information assets enable it to do. The board should provide the oversight necessary to ensure the organization has sufficient capability and agility to meet the marketplace dynamics.

8. Do the board and management know and understand the value of the organization's information assets?

For many organizations information assets can be one of, if not the most, significant determinants of the overall value of the organization. While some of those information assets are physical and tangible (e.g., computers, servers, etc.), most of them are intangible and typically not reflected on the balance sheet. Furthermore organizations usually do not track those intangible assets in their asset management systems. An organization's information assets include:

- Traditional fixed assets related to information management and processing including hardware, software, etc.
- Intellectual property including not only patents, trademarks and copyrights, but also business methods, processes and systems; product formulations and recipes or bills of materials; engineering diagrams, manufacturing methods, etc.
- Supplier, customer and business-partner relationships, contracts and agreements
- Training programs, employee skills, competencies, capabilities and knowledge of the organization, its products, processes and relationships
- Historical knowledge and intelligence, typically encapsulated in business and transaction data, data warehouses and business intelligence systems
- Organizational expertise and capabilities such as product innovation, design, engineering, manufacturing, distribution, etc.

Data warehousing and business intelligence systems have been available for some time, but organizations are still struggling with getting meaningful information out of the volumes of data that are available. Content- and knowledge-management systems are emerging and evolving in their capabilities to capture, store and provide access to corporate information and knowledge. However for the most part, approaches and techniques for inventorying, cataloguing and valuing the organization's information assets are in their infancy. In spite of these challenges however, as information assets continue to increase in importance to the organization's success, it is critical for organizations to have better awareness of what its information assets are and how to derive value from those assets.

Management should be inventorying and cataloguing the organization's information assets, and developing strategies, plans and accountabilities to preserve and enhance the value of those assets. Information for some assets, such as hardware, software and patent holdings, may already be available (at least historical cost and amortization amounts). Management should continue to expand these inventories to include other classes of information assets. Value assessments and preservation and enhancement plans should consider such things as the expected duration or useful life of the assets, and value enhancement activities such as cleansing, replenishment, refreshment or replacement.

Many organizations only begin to think about their information assets as a reaction to corporate acquisition or divestiture opportunities. Especially for organizations operating in *Turnaround Mode* and *Strategic Mode* it is increasingly important to be proactive in identifying these assets to focus strategies for leveraging and maximizing their value.

9. How are the value and contribution provided by the organization's information assets defined and measured?

Previous questions have dealt with identifying and defining the organization's information assets and the importance of maximizing the value of

those assets. This question focuses on how the organization defines and measures the value that its information assets provide. Many organizations take a "cost-centre view" of information assets. This view can provide useful information on the costs associated with providing related services. It not only considers the capital and infrastructure costs but also the ongoing operational costs (sometimes referred to as the cost to "keep the lights on"). This approach may be appropriate for organizations operating in *Support Mode* or *Factory Mode* where ongoing operational costs would typically represent a high percentage of the total information-asset costs.

As the strategic importance and value of information assets increase (such as for companies operating more in *Turnaround Mode* or *Strategic Mode*) it becomes important to take an "investment view" and focus more on measuring the strategic contribution and return on investment. These measurements are based on the business value associated with the corresponding investments in information assets. Return on investment approaches are relatively common for significant information system projects, although they can be challenging due to the difficulty in measuring non-tangible benefits associated with these projects. Many organizations are adopting similar approaches for ongoing delivery of information services. For example, being able to determine the cost (or ongoing operating investment) to provide the organization's customer call-centre or help-desk services better enables the organization to assess the value derived relative to the ongoing investments those services require. Such an approach also enables better business decisions by giving the organization the ability to compare service costs and service levels to external organizations and services providers.

The Balanced Scorecard is another common approach organizations use to develop goals and monitor performance as distinct from a more holistic view of the organization's goals and objectives, beyond just financial measures.

In order to have more holistic measures for its information assets, it may be appropriate to apply techniques similar to the Balanced Scorecard to develop goals and measure performance of the organizations information systems and technologies. Exhibit 2 identifes a number of non-financial and non-technical elements that may be useful to measure the value and contribution of the organization's information assets. Such measures should be a component of, and integrated with the overall Balanced Scorecard used within the organization. The fundamental concept is that the value and contribution of the organization's information assets should include measures beyond the technical metrics normally used to measure technology performance.

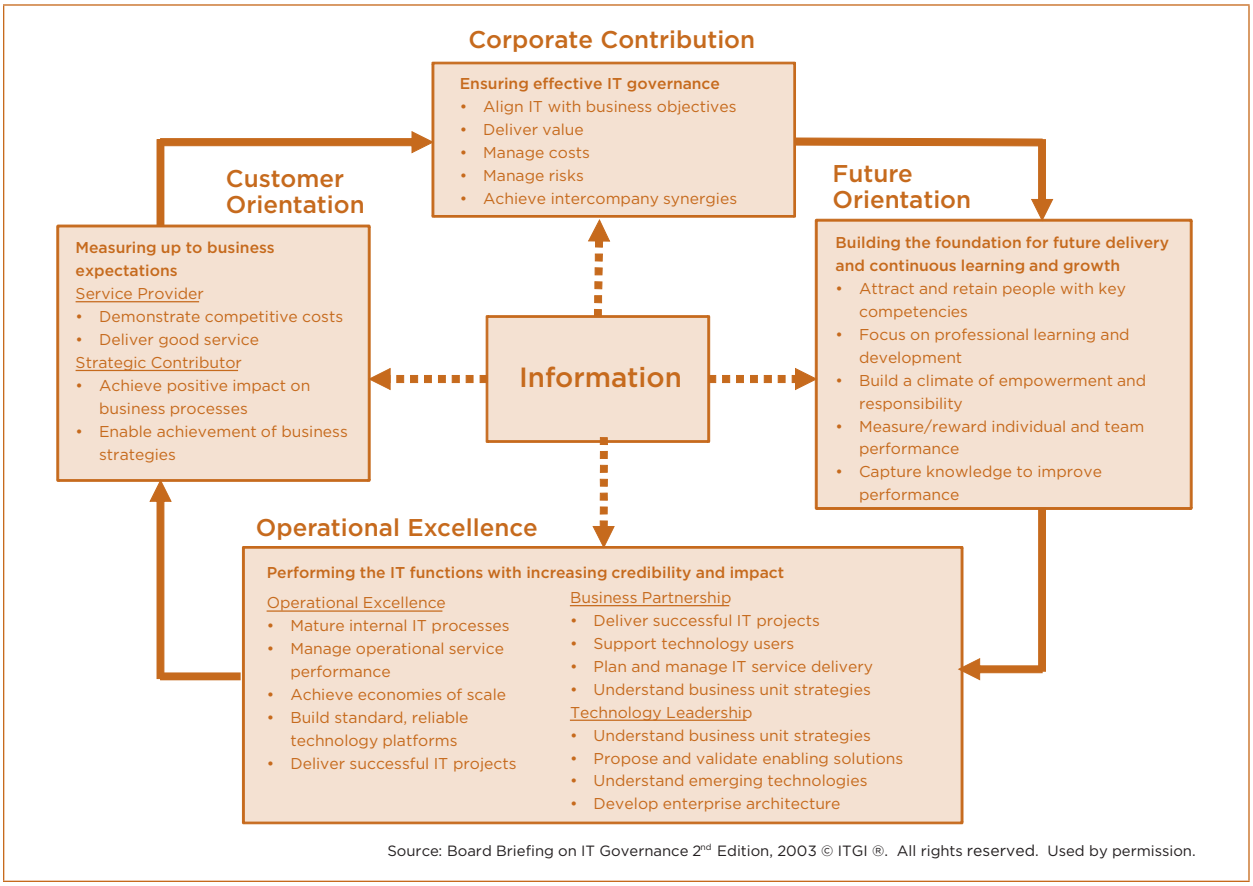
The key element related to this question is understanding how the organization defines and measures the contribution and value provided by its information assets in terms that are meaningful and important to the organization. They need to do it in a way that enables the board to provide the oversight and direction needed by management to ensure the value of these assets is maximized in the same way as other corporate assets.

10. How are emerging technologies and trends, and their potential impact on the organization monitored and assessed?

Technological innovation can present disruptive forces in the marketplace, displacing goods and services and creating entirely new business models. Portable devices and ubiquitous high-speed networking are changing employee and customer expectations about the way in which information is being captured, processed and distributed. Online marketplaces are changing the methods by which organizations interact with their customers, suppliers and business partners. Globally interconnected networks are facilitating access to global marketplaces and providing low-cost entry points for new competitors. Expansion of "pay-for-use" models for delivery of information services (such as cloud computing) are shrinking implementation and "time-to-market" lead times and are changing the economics of "peak-demand" processing and service delivery as a whole. Customer access to vast amounts of information and the increasing ease of finding competitive or substitute products is intensifying the competitive pressures. The emergence of sophisticated business-intelligence and knowledge-management tools can create competitive opportunities for those who are able to leverage the resulting business insights.

It is important for all organizations to understand and explore technological innovations and to

Exhibit 2 — Example IT Balanced Scorecard



monitor existing and new competitors and their use of technology. For organizations that are operating more in the *Support Mode* or *Factory Mode* it is important to understand how these innovations can reduce costs and improve service efficiency and reliability, and whether emerging trends and technologies present a risk of accelerated obsolescence of the 'current business model'. It is important to understand potential disruptions to the marketplace and the competitive landscape so that business strategies can be adopted to ensure the organization does not become redundant or obsolete. Not monitoring emerging trends and innovations would be the corporate equivalent of "sticking your head in the sand" and could have disastrous consequences.

For organizations operating in *Turnaround Mode* or *Strategic Mode*, it is critical to monitor and explore emerging trends and innovations, and invest appropriately in research and development to capitalize on these opportunities. For *Strategic Mode* organizations, emerging technologies and innovation can be key business-success drivers. The ability to capitalize on emerging technologies will help them achieve and maintain their competitive positioning. For *Turnaround Mode* organizations, technology innovation provides important opportunities for business transformations and improving competitive advantage.

Like any research and development activity, not all technological innovations will be successful or result in lasting business value. It is not always advisable to be on the "bleeding edge". Early adopters are not always able to maintain their early gains and advantages, and sometimes it may be more advantageous to be a fast follower. Organizations are more likely to be successful, however, when decisions about how and when to adapt to such marketplace changes are made proactively based on reasoned analysis rather than as a reaction to a crisis situation.

Part C – Governing Information Asset Management and Performance

Board direction and oversight of operational activities is an important component of overall governance activities. Effective involvement in and oversight of information-asset management and operational activities demonstrate the board's recognition of the importance of IT and establishes an important tone at the top.

"...when top managers understand the degree to which they must be accountable for technology, for project expenditures, and for monitoring return on investment from IT, they will do a better job of ensuring that critical systems function as promised."

Nolan and McFarlan

Key questions include:

11. Is there appropriate accountability for identifying, acquiring and deploying information assets and capabilities to meet the needs of the organization?
12. How is performance of the organization's information assets and capabilities measured, monitored and reported?
13. Is the investment in information assets meeting the business's requirements for information and processing capability?

11. Is there appropriate accountability for identifying, acquiring and deploying information assets and capabilities to meet the needs of the organization?

Accountabilities for the organizational acquisition and use of information assets should be shared between the business and IT and not be the sole domain of the organization's IT function. Clarity of these accountabilities is essential to ensure the effective and efficient use of resources and to maximize the value from information asset investments. Some of the key areas requiring clear definition of accountabilities include:

- **Maintaining and enforcing information-asset-related policies** – The pace of technological change and competitive pressures in the marketplace create a very dynamic environment. It is important that the organization's policies be responsive to changes and risks in the business and the technological environment. It is not unusual for organizations to adopt restrictive policies when faced with technological innovation (for example, prohibiting the use of social networking tools such as Facebook in the workplace). It is also not uncommon for organizations to adopt technological innovations and capabilities (such as permitting employees to use their personal devices for business purposes) without having a clear plan or protocol for deriving business value from those innovations. It is important that the business implications of such innovations be explored and appropriate policies adopted on a timely basis to capitalize on their advantages while managing the corresponding business risks.
- **Integrating information-asset goals with business objectives and initiatives to set organizational priorities** – Dynamic, rapidly changing environments create both opportunities and demands for limited organizational resources. It is important to have a clear definition of accountabilities and transparent processes for making decisions about the best use of limited resources. Mechanisms such as an executive steering committee (with representation from all business areas) can help ensure that appropriate goals and objectives are established and embedded in business strategies to structure initiatives to be undertaken that will maximize value for the organization as a whole.
- **Determining functionality and investment requirements for systems implementation projects** – Lack of clarity of business functionality requirements can lead to overinvestment in systems functionality that is not necessary or that never gets used. Failure to adequately consider ongoing operational costs, in addition to initial implementation costs, can result in investment requirements in excess of

original expectations. Clear accountabilities for defining functionality and investment requirements are necessary to optimize the organization's investment in information assets that deliver maximum business value.

- **Ownership of information assets and responsibilities for maximizing their value** – Information assets need to be used effectively to generate value to the organization. On its own, information provides little if any real value. It must be used and applied in the context of a business situation or opportunity to generate value. An application solution such as a Customer Relationship Management System will not generate organizational value unless it is used to strengthen customer relationships and generate new ones. Ownership of information assets is shared between the business and IT. IT will typically have ownership and accountability for the technological components. However, business management needs to take ownership of the business solution components and be accountable for leveraging those assets to maximize their value.
- **Defining business requirements, identifying and deploying solutions** – Management and business process owners are accountable for their business goals and objectives, and correspondingly need to be responsible for defining their business requirements for information and processing capability to enable them to achieve those goals and objectives. Making good business decisions requires timely access to accurate and reliable information. Business management needs to be responsible for defining requirements relating to timeliness, accuracy and reliability of information. They need to work with the IT team to identify appropriate solutions and effectively deploy those solutions to satisfy their requirements. Business management needs to be responsible for driving technology-enabled business initiatives and be accountable for their success.

12. How is performance of the organization's information assets and capabilities measured, monitored and reported?

While previous questions explore how the organization defines and measures the value of its information assets, this question focuses on how the organization measures and monitors the performance of its information assets and capabilities.

Management needs to establish performance objectives and targets for its information assets, and to implement effective processes and systems to measure and monitor actual performance against these targets. These processes and systems should be integrated with the other performance management systems of the organization to provide a consistent and holistic view of organizational performance.

- **What performance objectives and targets have been established for the information assets that are aligned with the organization's strategic goals and objectives?** Key performance indicators (KPIs) need to be defined for those activities that are critical for achieving those goals and objectives.
- **What information asset performance measurement systems and processes have been established to monitor KPIs and to provide early warning of where corrective action may be necessary to ensure objectives are achieved?** Management should have systems and processes in place to monitor and report on key indicators and ensure appropriate corrective action is taken when necessary.
- **What processes exist for defining and monitoring performance of service providers and business partners?** Delivery of information services to the organization often involves complex relationships with vendors and business partners that may involve a wide range of performance requirements such as:
  - outsourcing supplier contractual commitments and service-level agreements;
  - hardware and software supplier maintenance and service commitments; and
  - disaster recovery facility access and site-capability commitments.

  These relationships need to be regularly monitored and managed to ensure the performance expectations of the organization are being met.
- **What processes exist for monitoring compliance with policies?** The organization's policies establish standards and expectations with respect to how the organization conducts its affairs. Performance measurement and monitoring should include measuring and monitoring compliance with these policies.

- **How does the organization benchmark performance against peers, the industry and competitors?** Developing and measuring performance against internal targets and metrics provide useful information relative to goals and prior performance. It may also be useful to periodically benchmark the organization's performance against external metrics such as peer, industry or competitor performance. A vast array of information is available from commercial and proprietary sources to assist in benchmarking IT operational practices and performance as a way to identify performance improvement opportunities.

13. Is the investment in information assets meeting the business's requirements for information and processing capability?

While specific business requirements will vary widely from organization to organization, it is important for management to know whether its information assets are effective and efficient in meeting their business-specific requirements. Successful organizations use a variety of tools and techniques to measure the degree to which its business requirements are being satisfied. For example, some techniques can include:

- Regular monitoring of service-level agreements between IT as a provider of services and business functions and departments as users of those services. It is important that such agreements are not just technical measures, but are focused on the business requirements of the user.
- Periodic assessment of user satisfaction with the information services provided.
- Monitoring of customer and business partner satisfaction with services that are enabled by technology such as, for example, company websites, trading partner portals, order processing and fulfillment systems, and supply chain management systems.
- Monitoring the social and environmental impact of the organization's use of information assets and incorporating relevant aspects into the organization's corporate responsibility reporting.
- Reinvestment plans and funding for refreshing its information assets to maximize their value, extend their useful life, or capitalize on new innovations.

On the other hand, lack of effective communication between business and IT management can result in the business requirements for information and systems processing capability not being satisfied. This, in turn, can prevent the achievement of goals and objectives. Symptoms that indicate the organization's information-asset investments are not satisfying its business requirements could include:

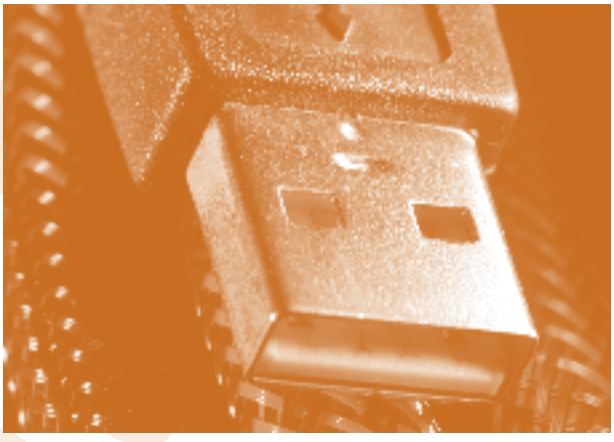
- Failed systems projects and projects that do not deliver their anticipated benefits. Such failures can indicate an inability to properly define business requirements and the benefits they will deliver, lack of effective project management, and/or inability to effectively implement solutions.
- Unmanageable backlog of change requests or resolution of reported problems.
- Extensive or uncontrolled user-developed applications such as spreadsheets and databases. Overdependence on these types of solutions can be symptomatic of user requirements not being satisfied through the normal acquisition and investment processes.
- Instances of "rogue" pay-per-use information services[6] (or cloud computing). Pay-per-use information services in themselves are not the issue. Such solutions can provide tremendous value to the organization. However, "rogue" instances (i.e., solutions adopted by users as a way to bypass normal procurement channels) may be indicative of the organization's information assets not meeting its business requirements.

6 The emergence of pay-per-use information services can fundamentally change the nature of investments in information assets from a traditional capital investment to an operating expense. For example, implementing a Customer Relationship Management system would traditionally involve an initial capital expenditure to acquire and deploy a solution, plus ongoing operating costs to maintain it. The emergence of online pay-per-use solutions (such as salesforce.com) enables organizations to replace the capital expenditure with a rate-per-user operating expense.

Part D – Governing the Organization's Information Asset Risks

Identification and management of the business risks associated with information assets is an integral component of the organization's overall risk management program. Part of the responsibility of the board is to oversee the organization's identification of its principal risks and the decisions and methods employed to manage them. However, for many organizations, the risk assessments and corresponding mitigation plans presented to the board are often too general with respect to the organization's information assets and use of information technologies.

The questions in this section are intended to provide board members with guidance with respect to the business risks associated with an organization's information assets. Regardless of the strategic importance of information assets to the organization, boards need to be satisfied that appropriate risk management strategies are in place and operating. However, the more strategically important its information assets are to the organization, the more important it is for the board to focus attention on the relevant information asset risks. Organizations operating on the Defensive side of the continuum would likely tend to focus board attention on risks related to information integrity and reliability, compliance requirements and ensuring the organization is keeping pace in the competitive marketplace. Availability risks become more significant for organizations operating in *Factory Mode*. On the Offensive side of the continuum, confidentiality risks as well as sufficiency and adequacy of resources become increasingly significant. In addition, ability to leverage and capitalize on emerging technology opportunities to achieve and sustain competitive advantage is also a key risk area.



Key questions include:

14. What measures are being taken to enhance, preserve and safeguard the integrity and reliability of the organization's information assets, commensurate with their importance and value?
15. How is the confidentiality of intellectual and information assets protected, commensurate with their importance and value?
16. Are there adequate plans and sufficient resources to provide the continued availability of information and processing capability to enable continuity of critical business operations?
17. How are legal, regulatory and contractual obligations related to information assets monitored for compliance?
18. Are there sufficient appropriate IT resources and competencies including succession plans for key IT personnel?
19. How does management ensure that its information and information resources, systems and technologies are keeping pace with changing business needs and enabling the organization's success?

14. What measures are being taken to enhance, preserve and safeguard the integrity and reliability of the organization's information assets, commensurate with their importance and value?

As discussed previously, information can be one of the most valuable assets of an organization. The value of that asset however, is directly related to its integrity and reliability. Information integrity is the representational faithfulness of the information to the underlying subject of that information, whereas reliability refers to the extent to which the information is appropriate, relevant, timely and meaningful.

Information Integrity and Reliability

*"**Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations."*

*"**Reliability**" relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities."*

IT Governance Institute

We have become so accustomed to automated information and information systems that it is easy to become complacent and assume information presented to us is accurate, complete and reliable.

It is important to remember that integrity and reliability of information and information systems is not automatic. To preserve, protect and enhance the value of its information assets it is important that the organization assess, prioritize and appropriately manage the risks that could impair their integrity and reliability. Organizations should have a comprehensive program of ongoing systemic risk review involving:

- Defining the integrity and reliability requirements of classes of information within the organization;
- Independent reviews of information-asset risk identification and assessment, and evaluation of risk management strategy sufficiency and effectiveness;
- Reviews of susceptibility and vulnerability to internal and external threats that could impact information-asset integrity and reliability;
- Review of assignment of access privileges to enforce effective segregation of responsibilities and to prevent or detect fraud; and
- Periodic information integrity audits.

15. How is the confidentiality of intellectual and information assets protected, commensurate with their importance and value?

The preservation of value derived from information is highly dependent on the organization's ability to protect the confidentiality of that information. Inappropriate disclosure of proprietary trade secrets, product recipes and formulations, and strategic business plans are just a few examples of how failure to appropriately protect confidentiality could have significant reputational and legal consequences for the organization. In some cases there are legal and regulatory requirements to maintain appropriate confidentiality of information. Examples include the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and contractual commitments to protect information by non-disclosure agreements.

Not all information requires the same degree of confidentiality. Contact information, for example needs to be shared to be of value. As part of its risk management program, it is important that organizations identify their information assets and the corresponding business requirements for confidentiality. The organization's privacy policies should include accountabilities and processes for protecting personally identifiable information. Its information security policies should include accountabilities and processes for determining information sensitivity and corresponding confidentiality requirements. Appropriate systems, processes and safeguards should be implemented to protect and preserve the privacy and confidentiality of sensitive information, and to quickly respond to incidents that may jeopardize that confidentiality.

16. Are there adequate plans and sufficient resources to provide the continued availability of information and processing capability to enable continuity of critical business operations?

Organizations depend on the availability of their information assets to conduct business and provide goods and services to their customers. But information assets are not infallible and are subject to human error, natural and man-made events and disruptions. It is typically impractical (if not impossible) and usually unnecessary to construct an entire information-systems infrastructure to be able to withstand all possible events. The challenge then for organizations is to:

- Identify critical business operations and define a minimum level of acceptable service for those operations. Business managers need to balance the costs of maintaining service levels with the potential business impact of not being able to provide that level of service.

- Identify the information assets required to enable those critical business operations to provide the minimum level of acceptable service.
- Develop business plans for maintaining the defined level of acceptable service for those critical business operations (often referred to as a Business Continuity Plan) and integrate them with IT plans for providing the necessary information assets (referred to as an IT Service Continuity Plan).
- Identify and train the people necessary to execute both the Business and IT Service Continuity Plans.
- Regularly test and exercise those plans (and the people) to ensure their capability, sufficiency and viability.
- Review, revise and update the plans to retain their effectiveness, accommodate additional disruption scenarios, and to reflect changes in critical business operations and minimum levels of acceptable service.

The essential element for maintaining an effective and efficient plan for the continued availability of information assets is to make sure the plan is based on and responsive to ensuring the business is able to provide its defined minimum level of acceptable service.

The terms Business Continuity Plan and IT Service Continuity Plan are being increasingly used to replace the historical term Disaster Recovery Plan to reflect the need to maintain continuous service rather than to recover from a disruption of service.

17. How are legal, regulatory and contractual obligations related to information assets monitored for compliance?

Board members should receive information from management that satisfies them that legal, regulatory and contractual obligations and commitments related to its information assets are identified and that compliance is appropriately measured and monitored.

Examples of legal, regulatory and contractual obligations could include:

- Assessment of the sufficiency and operating effectiveness of controls over accuracy of financial information and appropriateness of access to that information as required under public company CEO/CFO certification legislation
- Protection, proper use and destruction of personally identifiable information under privacy legislation
- Commitments to protect and maintain proprietary-information confidentiality under vendor, customer and trading-partner contractual agreements
- Computer hardware and software user licensing requirements
- Obligations and commitments under outsourcing agreements or other third-party service arrangements
- Industry-specific regulatory requirements for such things as information system recovery, or restrictions on cross-border transmission and storage of data.

Contracts, such as cloud computing, long-term outsourcing service agreements, etc., can be very complex, include significant commitments over long periods of time and potentially expose the organization to hidden risks, including the lack of appropriate security, availability or other controls. Legislative and regulatory requirements can be similarly complex and, in some cases contradictory between jurisdictions and perhaps within a given jurisdiction. The board should be satisfied that management has followed due process and employed the appropriate skills, advice and legal counsel as part of negotiating its contractual commitments and for understanding its legislative and regulatory obligations.

Management's processes for identifying and monitoring compliance with obligations and commitments related to its information assets should be effectively integrated with the enterprise risk management and compliance management program. Timely monitoring and reporting to the board can enhance the culture of the organization by demonstrating support and encouraging compliance.

In measuring and monitoring compliance, a distinction should be drawn between oversight of non-compliance incident investigations and seeking assurance that the systems and processes surrounding the compliance program are effective. Both of these activities have their place. Most organizations recognize the need to investigate non-compliance events and report significant items to the board. Fewer organizations dedicate themselves to systemic learning from these incidents (that may

indicate improvement opportunities for their risk management and compliance programs), or subject their programs to rigorous external review.

18. Are there sufficient appropriate IT resources and competencies including succession plans for key IT personnel?

Organizations need sufficient IT resources with the appropriate skills not only to operate and manage existing information processing capabilities, but also to deploy appropriate new and emerging capabilities. The board should be satisfied that the organization has sufficient and appropriate IT resources and competencies to meet its current and future business requirements. It should consider such things as:

- periodic management reviews of skill and competency requirements and their incorporation into relevant job descriptions and organizational structures;
- sufficiency of existing resources, adequacy of competencies and the status of recruiting efforts in key skill areas such as emerging technologies, internal audit, risk management and compliance;
- nature and adequacy of training and development programs to maintain and develop appropriate skills in emerging areas;
- nature and adequacy of user training and support programs to enable efficient, effective and appropriate use of the organization's information and information systems; and
- nature and status of succession planning for key IT personnel.

Maintaining sufficient resources with appropriate competencies is an essential requirement to ensure the organization's requirements for information and information systems are sufficient to maintain its competitive positioning and to capitalize on opportunities in the marketplace.

19. How does management ensure that its information and information resources, systems and technologies are keeping pace with changing business needs and enabling the organization's success?

Keeping pace with the evolution of information technologies can very much feel like "it takes all the running you can do, to keep in the same place". But keeping pace is important for all organizations, including those in *Support Mode* and *Factory Mode* or they risk becoming redundant or obsolete. For *Turnaround Mode* and *Strategic Mode* organizations, they may very well need to "run at least twice as fast as that" to enable the transformations necessary to improve their competitive positioning or to maintain their leadership role. Boards need to provide direction and oversight of management to be satisfied the organization is taking appropriate measures to ensure that its information assets keep pace with the organization's changing business needs.

> "Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"
>
> The Red Queen in Through the Looking-Glass, by Lewis Carroll

Some of the qualities and practices of leading organizations include:

- IT leadership that understands the business, is capable of effective communication in terms the business can understand, and is actively and meaningfully engaged as a member of the executive management team;
- regular awareness sessions for executive management on the business impact of emerging technologies;
- integration of IT with the strategic and business planning process and, just as importantly, integration of business management in IT planning processes;
- executive management awareness of and accountability for:
  - the business impact and value delivered by technology-enabled business processes and initiatives,
  - identifying and managing the business risks related to its information assets;
- structured and planned investment in research and development activities exploring the business potential of new and emerging technologies;
- active maintenance of corporate policies to ensure they are appropriate to enable business success but do not serve as a barrier to innovation.

Part E – The Board's Use of Information and Information Systems

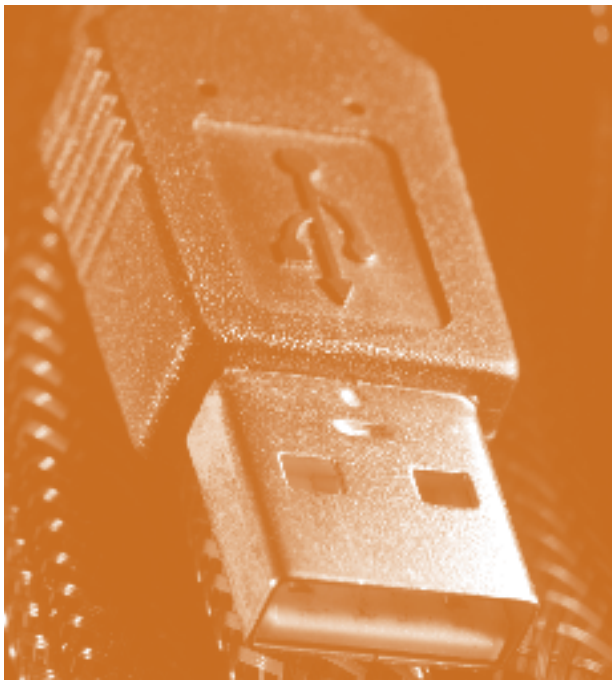
So far, the questions have dealt with the governance role of the board. However, the board is also active in creating and using information on behalf of the organization and, as such, has a user role. This question involves the board members assessing their own use of information assets to improve their efficiency and effectiveness and the value they provide to the organization.

20. How does the board leverage information technology to improve the board's value and the efficiency and effectiveness of its operations?

The board is not just a recipient of information provided by management; it is an integral component of an organization's governance and communication infrastructure and, as such, performs activities that create, transform and use information. Accordingly, board members should be aware and look for opportunities to leverage the organization's information assets to improve the board's efficiency and effectiveness and to add shareholder value.

Opportunities for boards to deploy and use information assets include:

- **Information portals and document management systems** – The board can use these to facilitate distribution of board materials and information packages in a more efficient and cost-effective manner. The portals could be used not only to disseminate board packages, but also to provide access to external information such as industry updates, legal and regulatory changes, etc.
- **Dashboards and executive information systems** – These can provide more accurate and timely information at a level of detail that is appropriate for consumption at the board level. Executive management has implemented such systems to provide themselves with information at the appropriate level of detail to enable them to monitor business operations. Board reporting should also be considered as part of the business requirements of these systems. Such systems should provide relevant alerts and facilitate board-level monitoring of financial and operational performance as well as monitoring other governance-related activities such as compliance reporting, audit findings, whistleblower activities, regulatory findings, privacy incidents, risk management program status, etc.
- **Use of mobile and telecommunication technologies** – Smartphones, tablets and laptops, audio-video teleconferencing and virtual meetings can facilitate meetings and communications between board members and between the board and management.
- **Use of Internet technologies** – Webcasting, blogs, collaboration tools, and other social networking mechanisms can facilitate communication between board members and between the board and the organization's stakeholders.



As with other organizational uses of its information assets, information shared at the board level can contain highly confidential and sensitive information. Appropriate assessment of the risks and security requirements of this information needs to be considered and appropriate measures put into place to ensure the integrity, security and confidentiality of this information.

Appendix 1–Sample Board IT Governance Calendar

ISO 38500 suggests three primary tasks through which board members should fulfil this responsibility with respect to information and related technologies:

a. **Evaluate** the current and future use of the organization's information and information systems, resources and technologies
b. **Direct** preparation and implementation of plans and policies to ensure that use of the organization's information assets meets business objectives
c. **Monitor** conformance to policies, and performance against the plans.

The table below is an example of a Board IT Governance Calendar that can be used to identify specific activities the board may choose to undertake (either at the board level with committees of the board) and a suggested frequency of those activities. A cross-reference is provided to the relevant questions boards should ask as outlined in this document. The table suggests varying the frequency of activity depending on the board's assessment of the strategic importance of information assets to the organization as discussed further in Question 1. Governance activities will, of necessity, vary significantly between organizations. The activities and frequency suggested in this table are presented only as guides. Boards should develop specific activities and frequencies as appropriate for their unique circumstances. Further, the activities presented here focus primarily on matters related specifically to information and technology. Many of these activities may be encompassed within other board activities. For example, reviewing the appropriateness of board skills, competencies and capabilities related to information and technology would typically be conducted as part of the board's overall review of its skills and competencies, and not necessarily as a separate activity.

Board IT Governance Calendar	Cross-Reference to Relevant Question	Organizational Positioning on IT Strategic Impact Grid	
		Defensive	Offensive
Evaluate			
Re-assess strategic importance of IT to the organization	1	Annually	Annually
Review and assess adequacy of board role with respect to governance of the organization's information assets	2	Annually	Annually
Review appropriateness of board skills, competencies and capabilities	3	Annually	Annually
Receive information from internal sources, outside experts and from other companies regarding the business implications of emerging technologies, technology approaches and strategies	3/10/19	As needed	Annually
Review appropriateness of the organization's information asset strategy and alignment with business strategies	5	Annually	Annually
Review effectiveness and efficiency of board use of information technologies	20	As needed	Annually
Direct			
Review and approve goals and objectives for information asset performance (incorporated into business goals, objectives and plans)	12	Annually	Annually
Review roles, responsibilities and accountabilities for information asset strategies and initiatives	6	As needed	As needed
Review business case and value proposition for strategic projects	9	As needed	As needed
Review sufficiency and appropriateness of information reported to the board	4	Annually	Annually
Review management approach to identifying and valuing the organization's information assets	8/9	Annually	Annually
Review roles, responsibilities and accountabilities for information asset acquisition and deployment	11	As needed	As needed
Review adequacy and appropriateness of information asset related policies	11/19	As needed	Annually
Review identification and assessment of information asset related business risks	14/15/16/17/18/19	Annually	Annually
Monitor			
Review management assessments of the sufficiency and appropriateness of the organization's information assets, resources and capabilities	7	As needed	Annually
Review significant changes to the organization's information assets	8	As needed	As needed
Monitor organizational performance compared to identified goals and objectives	12	As needed	Monthly
Receive and review updates on strategic projects	12	As needed	Quarterly
Monitor user, customer and stakeholder feedback on satisfaction with services enabled by technology	13	Annually	Quarterly
Review internal control assessments and critique action plans	14/15/16/17/18	As needed	Annually
Review and appraise IT service continuity capability	16	Annually	Annually
Review and monitor management action plans with respect to significant non-compliance incidents	17	As needed	As needed
Review internal audit and third party audit findings and monitor status of management action plans	14/15/16/17/18	As needed	Quarterly
Review development and succession plans for key IT resources	18	As needed	Annually
Receive management assertions related to contractual, legal and regulatory compliance	17	Annually	Annually

Appendix 2 – IT Governance Frameworks

There are a number of popular frameworks that have been published to provide guidance to boards and management on concepts, approaches and techniques to improve the governance and management of information and information resources, systems and technology. In this appendix we introduce three such frameworks.

IT Governance Focus Areas – IT Governance Institute, 2003

In this publication, the IT Governance Institute indicates that IT governance is concerned with two things: (1) IT's delivery of value to the business and (2) mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the desired results are obtained.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: ***Value Delivery*** and ***Risk Management***. Three of them are drivers: ***Strategic Alignment***, ***Resource Management*** and ***Performance Measurement***.

For additional information on the five main focus areas for IT governance, see *Board Briefing on IT Governance*, 2nd Edition, by the IT Governance Institute.

COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT

COBIT 5 is the latest edition of ISACA's globally accepted framework, providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises. The COBIT 5 process reference model divides the governance and management processes of enterprise IT into two main process domains – governance and management. It represents all the processes normally found in an enterprise relating to IT activities and provides a common reference model understandable to operational IT and business managers. The governance domain contains the following five governance processes:

- Define/Maintain Governance Framework
- Value Realization/Optimization
- Resource Utilization/Optimization
- Risk Optimization
- Stakeholder Transparency

Within each process, the practices of evaluating, directing and monitoring are defined.

COBIT 5 is available from ISACA at http://www.isaca.org/COBIT/Pages/default.aspx

ISO\IEC 38500: 2008 - Framework for Good Governance of IT

ISO/IEC 38500 *Corporate Governance of Information Technology* is an international standard for corporate governance of information technology published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.

The framework comprises definitions, principles and a model. It sets out six principles for good corporate governance of IT responsibility, strategy, acquisition, performance, conformance and human behaviour. The principles express the preferred behaviour to guide decision making.

The framework also includes a model for corporate governance of IT defining the three main tasks: evaluate, direct and monitor, which were discussed previously in Appendix 1.

Bibliography

Bart, C. & Turel, O. 2010. "IT and the Board of Directors: An Empirical Investigation into the 'Governance Questions' Canadian Board Members Ask about IT.", Journal of Information Systems, 24(2): 147-172

Boston Consulting Group, "BCG Matrix - Meaning and its Limitations." (n.d.). Retrieved April 8, 2012, from http://www.managementstudyguide.com/bcg-matrix.htm

BSI Group. 2008. "BS ISO/IEC 38500:2008 - Corporate governance of information technology." www.bsigroup.com/standards

Butler, R. & Butler, M.J. 2010. "Beyond King III: Assigning accountability for IT governance in South African enterprises." S.Afr.J.Bus.Manage, 41(3): 33-45

Canadian Institute of Chartered Accountants. January 2012. "Director Alert - Social Media – questions for directors to ask." http://www.cica.ca/DirectorsQuestions-SocialMedia. CICA Risk Oversight and Governance Board

Canadian Institute of Chartered Accountants. March 2012. "Role of Social Media in Performance Reporting – A Discussion Brief." http://www.cica.ca/PerformanceReporting-SocialMedia. CICA Canadian Performance Reporting Board (CPRB) and the Canadian Investor Relations Institute (CIRI)

Canadian Securities Administrators. 2005. "National Policy 58-201 Corporate Governance Guidelines."

Corporate Board Member. 2007. "2007 Board and Information Technology Strategies Report: MAXIMIZING PERFORMANCE THROUGH IT STRATEGY Eight Big Ideas from the Corporate Board Member/Deloitte Touche Tohmatsu Survey on Information Technology in the Boardroom." Special Supplement. Corporate Board Member magazine. Brentwood, TN

Datardina, M. and Audette, Y. 2011. "ITAC Brief – Cloud Computing: A Primer." Canadian Institute of Chartered Accountants

Datardina, M and Parker, R. 2011. "The top ten tech issues." CAmagazine.com. (Sept 2011). Retrieved June 27, 2012, from http://www.camagazine.com/archives/print-edition/2011/sep/features/camagazine51661.aspx

Deloitte Consulting LLP. 2006. "What the Board Needs to Know about IT: Phase I - The board's role in leveraging technology as a strategic resource". Deloitte & Touche LLP

De Haes, S. & Van Grembergen, W. 2008. "An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment", Information Systems Management, 26: 123–137

ISACA. 2012. COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, Il

IT Governance Institute. 2003. *Board Briefing on IT Governance*. 2nd Edition. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx

Jewer, Dr. Jennifer. 2009. "Drivers and Performance Outcomes of Board Information Technology Governance – Participants Report". University of Waterloo

McCarthy, Mary Pat, and Steven Hill. “Don’t Forget the ‘Offensive’ Side of IT Risk.” Directorship. Boardroom Intelligence. http://www.directorship.com/don’t-forget-the-“offensive”-side-of-it-risk/

McCarthy, Mary Pat, and Sanjaya Krishna. “Social Media: Time for a Governance Framework.” Directorship. Boardroom Intelligence. http://www.directorship.com/social-media-time-for-a-governance-framework/.

McFarlan, F.W. 1984. “Information technology changes the way you compete.” Harvard Business Review, May-June 1984: 98-103

Nolan, R. and McFarlan, F.W. 2005. “Information Technology and the Board of Directors.” Harvard Business Review, October

Peppard and Ward, 2004. “Beyond strategic Information systems: towards an IS capability.” Journal of Strategic Information Systems. v13 i2. 167-194

Parent, M. & Reich, B. H. 2009. “Governing Information Technology Risk.” California Management Review, 51(3): 134-152

Posthums, S., von Solms, R., King, M. 2010. “The board and IT governance: The what, who and how.”, S.Afr.J.Bus.Manage, 41(3): 23-32

Raghupathi, W. 2007. “Corporate Governance of IT: A framework for development.” Communications of the ACM, 50(8): 94-99

Travica, Bob. *The Design of the Virtual Organisation*. http://home.cc.umanitoba.ca/-btravica/voais.html. (1997)

Zukis, Bob. “Boards and a Social Networking-Driven Future.” Directorship. Boardroom Intelligence. http://www.directorship.com/boards-and-a-social-networking-driven-future/

Where to find more information

CICA Publications on Governance*

The Director Series

The 20 Questions Series

20 Questions Directors and Audit Committees Should Ask about IFRS Conversions (Revised)
20 Questions Directors Should Ask about Building a Board
20 Questions Directors Should Ask about CEO Succession
20 Questions Directors Should Ask about Codes of Conduct (2nd ed)
20 Questions Directors Should Ask about Crisis Management
20 Questions Directors Should Ask about Crown Corporation Governance
20 Questions Directors Should Ask about Director Compensation
20 Questions Directors Should Ask about Directors' and Officers' Liability Indemnification and Insurance
20 Questions Directors Should Ask about Executive Compensation (2nd ed)
20 Questions Directors Should Ask about Governance Assessments
20 Questions Directors Should Ask about Governance Committees
20 Questions Directors Should Ask about Insolvency
20 Questions Directors Should Ask about Internal Audit (2nd ed)
20 Questions Directors Should Ask about IT (2nd ed)
20 Questions Directors Should Ask about Management's Discussion and Analysis (2nd ed)
20 Questions Directors Should Ask about Responding to Allegations of Corporate Wrongdoing
20 Questions Directors Should Ask about Risk (2nd ed)
20 Questions Directors Should Ask about the Role of the Human Resources and Compensation Committee
20 Questions Directors Should Ask about their Role in Pension Governance
20 Questions Directors Should Ask about Special Committees (2nd ed)
20 Questions Directors Should Ask about Strategy (3rd ed)

Director Briefings

A Framework for Board Oversight of Enterprise Risk
Climate Change Briefing — Questions for Directors to Ask
Controlled Companies Briefing — Questions for Directors to Ask
Diversity Briefing — Questions for Directors to Ask
Long-term Performance Briefing — Questions for Directors to Ask
Shareholder Engagement – Questions for Directors to Ask
Sustainability: Environmental and Social Issues Briefing – Questions for Directors to Ask

Director Alerts

The ABCP Liquidity Crunch — questions directors should ask
Executive Compensation Disclosure — questions directors should ask
Fraud Risk in Difficult Economic Times — questions for directors to ask
The Global Financial Meltdown — questions for directors to ask
Human Resource and Compensation Issues during the Financial Crisis — questions for directors to ask
New Canadian Auditing Standards — questions directors should ask
Social Media – questions for directors to ask

The Not-for-Profit Director Series

NPO 20 Questions Series

20 Questions Directors of Not-for-Profit Organizations Should Ask about Board Recruitment, Development and Assessment
20 Questions Directors of Not-for-Profit Organizations Should Ask about Fiduciary Duty
20 Questions Directors of Not-for-Profit Organizations Should Ask about Governance
20 Questions Directors of Not-for-Profit Organizations Should Ask about Human Resources
20 Questions Directors of Not-for-Profit Organizations Should Ask about Risk
20 Questions Directors of Not-for-Profit Organizations Should Ask about Strategy and Planning
Liability Indemnification and Insurance for Directors of Not-for-Profit Organizations

NPO Director Alerts

Pandemic Preparation and Response — questions for directors to ask
Increasing Public Scrutiny of Not-for-Profit Organizations — questions for directors to ask
New rules for charities' fundraising expenses and program spending — questions for directors to ask
New Accounting Standards for Not-for-Profit Organizations – questions for directors to ask
The New Canada Not-For-Profit Corporations Act – questions for directors to ask

Other Publications

A Guide to Financial Statements of Not-For-Profit Organizations – questions for directors to ask
Accountants on Board — A guide to becoming a director of a not-for-profit organization

The CFO Series

Deciding to Go Public: What CFOs Need to Know
Financial Aspects of Governance: What Boards Should Expect from CFOs
How CFOs are Adapting to Today's Realities
IFRS Conversions: What CFOs Need to Know and Do
Risk Management: What Boards Should Expect from CFOs
Strategic Planning: What Boards Should Expect from CFOs

*Available at www.rogb.ca.

About the author

Gary S. Baker, BBA, CA, CGEIT

Gary S. Baker is an independent consultant, with more than twenty-five years experience providing IT governance, risk management and internal controls consulting services and advice. He was formerly the Canadian IT Governance service offering leader for a multinational professional services firm. Gary is a graduate of Wilfrid Laurier University with an Honours Bachelor of Business Administration and is a Chartered Accountant. He is certified in the Governance of Enterprise Information Technology, and holds Foundation level certificates in ITIL and COBIT 4.1. Gary is a lecturer in the University of Waterloo's School of Accounting and Finance and currently serves on the CICA's IT Advisory Committee and the CICA/AICPA Trust Services Task Force. Gary was a participant in the ISACA COBIT 5 Development workshops and has previously served on ISACA's COBIT Steering Committee and the ISACA COBIT Enterprise Certification Task Force.

20 Questions Directors Should Ask about **IT**

Second edition

277 Wellington Street West
Toronto, ON Canada M5V 3H2
416.977.3222 www.cica.ca