Governering Information Technology Risk

Michael Parent
Blaize Horner Reich
When information systems or technology fail, they often cause significant impacts on shareholder value. For example, early in 2001, Canada’s second-largest grocery retailer, Sobeys Inc., abandoned an $89 million SAP implementation, taking an after-tax charge of $49.9 million, or $0.82 per share. Sydney Water, a public utilities company in Australia, abandoned a customer relationship management and billing system in 2002, with an estimated write off of AUD$61 million. The auditor-general for New South Wales wrote a scathing report, criticizing its Board for failing to exercise proper oversight. In 2005, U.S. credential verification service provider ChoicePoint publicly admitted to inadvertently providing over 150,000 names, addresses and other sensitive information to criminals. In 2007, The TJX Companies, Inc. (the owner of T.J. Maxx, Marshall’s, and other stores in North America and the UK) was on the defensive after customer data, including credit and debit card information, was stolen from their systems and used fraudulently.

McAfee underlines the importance of IT investment, asserting that U.S. companies spend as much on information technology each year as they do on offices, warehouses, and factories combined. As a result of these large investments, the consequences of any disasters are likely to be profound and lasting. As Cavusoglu, Mishra, and Raghunathan showed, firms that experienced Internet security breaches subsequently lost an average of 2.1 percent of their market value within two days, resulting in a loss in market capitalization of over $1.6 billion each. TJX saw an initial short-term drop of 1.7 percent in stock price on January 30th, 12 days after the security breach was announced. Its stock took a further 3.6% drop two days later in response to a class action lawsuit and a call for the Federal Trade Commission to investigate TJX for possible negligence. While their stock eventually rebounded, and has gone on to outperform their
competitors’, this only occurred after an extensive and expensive advertising campaign that consumed management time and attention that would otherwise have been spent on improving their core business.

We see no sign that the pace and size of IT investments will abate, nor that IT-based risk will cease to be a problem. The 2005 CSI-FBI Computer Crime and Security Survey found that organizations remain reluctant to report security breaches because of a concern over the effect of negative publicity.\(^8\) Paradoxically, these same organizations also report believing that they do not invest enough in security, including cyber-insurance. This underscores the importance for Boards to act and act now if their companies are to minimize the effects of an ever-growing array of potential IT disasters.

Klinke and Renn suggest a three-step process to manage systemic risk: identify risk classes, create evaluation criteria, and design management strategies.\(^9\) This article addresses these three elements, at the Board of Directors level, to manage the risk emanating from information technology investments. Our review of the general topics of corporate governance and IT governance shows that a gap exists in this area. We introduce a chain of accountability, called the IT Risk Governance chain, which begins to address this gap by outlining what directors must do, at a minimum, to discharge their fiduciary responsibilities towards IT investments. Five major areas of IT risk are identified and discussed, and directors are provided with a dashboard of ten critical questions. On the whole, this framework represents the minimum level of attention Boards should pay to information technology investments in their organizations.

**Methodology**

Our interest in IT Risk Governance began when we, as Board members and Board educators realized that there was a dearth of practical advice concerning the governance of IT risk. Our review of the existing academic and practitioner literatures revealed that, while there was a growing body of literature on IT governance, it was aimed mainly at senior company managers. We found no framework or approaches that addressed the needs of the Board of Directors. Those studies that did examine the role of the Board in governing IT noted that Boards did not spend sufficient time on IT issues and their discussions are limited both in terms of scope and depth. They recommended that Boards should attend to IT issues in their organizations more thoroughly and judiciously. However, these studies fell short in suggesting to directors how they might do so without having to devote an inordinate amount of time, energy, and effort. Our research followed a 3-step process recommended by Yin\(^10\) and by Stake.\(^11\) After a review of the literature, we designed a multiple case study and set criteria for suitable
organizations. Given the novelty of our exploration, we decided to focus on established (not new or emerging) medium-to-large listed corporations with stable Boards of Directors. Our choice to focus on medium-to-large businesses was based on our perception that they would have larger Boards, hence more potential directors to interview. Being listed (with stocks trading on one or more exchanges), companies gave us access to public filings, annual reports, and other secondary source documents. It also meant that these organizations would comply with governance regulations in their respective jurisdictions (e.g., the SOX Act that dictates an external Chair and external directors for the audit committee). Finally, stable Boards meant that they had established governance processes that could be examined.

Using contacts gleaned from over 30 years as senior IT practitioners and academics, we recruited a total of 6 firms to this exploratory research project. They are described in Appendix 1. In each case, we were provided access to the Board and to their external directors. We conducted in-depth interviews with directors from each organization. These interviews were semi-structured and exploratory in nature, focusing on directors’ perceptions of the importance of IT issues in their organizations, their comfort in dealing with these issues, and where they felt attention needed to be paid when dealing with IT issues at the Board level. Concurrently, we reviewed all available secondary-source documents for evidence of attention to IT issues at the Board. This included annual reports, proxy statements, auditors’ reports, and where permitted, minutes from Board meetings.

Our analysis of the data from interviews and secondary documents was done in two phases. In the first, we reviewed interview transcripts to identify broad themes and possible constructs (construct elicitation). This was done iteratively and to the point of theoretical saturation, that is, until no new themes emerged. We then revisited the transcripts and archival data in a second round and conducted a content analysis to group the themes into categories. Five such themes emerged that led us to develop a preliminary version of the IT Risk Governance framework in Figure 2A.

The second phase of our analysis consisted of member checks where we sought preliminary validation of this model from the interview respondents. We shared the preliminary model and our analysis with the participants in the study and asked for their comments. Specifically, we were interested in their comments on the relevance of the five themes, on their completeness, and on whether any addition, deletions, or modifications were necessary. Some minor comments were made, and we incorporated these into the model. However, the final framework as presented in Figure 2B remained substantively unchanged and composed of the five factors we first identified.

**Corporate Governance**

Much has been written about governance and the role of the Board. Shailer defines governance as “decision making in the exercise of authority for
direction and control.” This definition implies four interrelated principles: first, directors know the strategic direction the company is pursuing; second, they act, or make decisions; third, directors hold ultimate authority over the affairs of the organization; and finally, directors’ duty-of-care centers on oversight and control.

Gillan suggests that corporate governance consists of a set of mechanisms internal and external to the firm. The former includes control systems (e.g., policies and procedures, information systems) that enable regulatory compliance. Directors need to exercise wisdom and foresight in discharging their duty of care. Boards fail in these duties through incompetence, which leads to civil penalties, and/or dishonesty, which has criminal consequences. As Nader stated over 20 years ago, “It is abundantly apparent that Boards of Directors can no longer operate with the slogan of ‘confidence in management.’”

**Information Technology Governance**

Information technology governance is a sub-set of the overall governance responsibilities of Boards and refers to decisions about key IT activities and investments in organizations. Weill and Ross define it as “the decision rights and accountability framework to encourage desirable behavior in using IT.”

There is ample evidence to suggest that, just as IT can create corporate wealth, it can also destroy it. According to The Standish Group, 30-40% of information systems (IS) projects experience escalation, with cost overruns averaging 43-189%. Clegg et al. assert that 80-90% of all IS investments fail to meet their performance objectives as a result of senior managers’ inability and/or unwillingness to exercise oversight over technology projects. Studies have shown that IT represents about one-third of all capital spending and the average enterprise’s IT investment is now greater than 4.2% of annual revenues.

Unfortunately, many Boards pay little, if any, attention to IT investments, and they do not concern themselves with minimizing potential waste or risk in this area. As Huff, Maher, and Munro found, Boards seem to be suffering from an IT attention deficit. Their study of 17 medium-to-large sized company Boards in the financial services and primary industry sectors revealed that just over half the Boards paid attention to information technology. Only two Boards reported discussing IT’s contribution to their competitiveness.

A recent study of 400 directors by Deloitte Consulting found many paradoxes: a huge majority recognizes that IT is important to success, but only 14% are actively involved in IT strategy. Sixty-six percent say IT should be discussed at the Board level but only 11% report a discussion at each meeting.

These studies have reported various causes for Board inattention. Although directors pinned the blame on the IT strategy or lack of alignment between the strategy and the business, other research suggests a lack of IT experience or competence in the boardroom, either collectively on the Board team and its internal and external advisors or individually on the part of its directors. This lack of interest and competence in IT is widespread, even among
technology company Boards. As Guldentops summarizes, “information technology has become a critical driver of business success, Boards of Directors have not kept pace. . . . oversight has often been lacking because IT has been seen as an operations matter, and Board members lacked interest or expertise in technology issues.”

Another reason might be the plethora of detailed IT frameworks that compete for directors’ attention. Appendix 2 (adapted from Webb, Pollard, and Ridley) lists over a dozen models to guide the governance of IT. Each model and method has its purpose and strengths, but none give clear, unambiguous guidance to Board members about participating effectively in IT governance,

Boards have increasingly relied on key informants, such as the CIO or external auditors. In doing so, they do not seem to seek details, but rather a guarantee or reassurance from “an expert” that all is “OK.”

**Two Types of IT Governance**

Business literature suggests that there are two parts to IT Governance. A passage from the IT Governance Institute states: “Fundamentally, IT governance is concerned about two things: IT’s delivery of value to the business and 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.”

Filatotchev suggests that the dominant view of Boards comes from agency theory, which emphasizes monitoring and control functions. Within this perspective, Directors responsibilities take two forms: ensuring accountability to minimize downside risk; and enabling managerial entrepreneurship to reap upside potential. These two perspectives are called the wealth-protecting and wealth-creating aspects of corporate governance. They see to it that wealth is not squandered or put at risk and ensure that measures are taken to increase this wealth over time. These two duties result in two forms of IT Governance. In its first, defensive form, IT governance exists to prevent IT-based catastrophes, or if they occur, to minimize their consequences to the business. We call this *IT Risk Governance*. The second form of IT governance is wealth-creating in nature and the result of strong IT strategic alignment. It leverages IT-based assets to increase shareholder value. We call this *IT Value Governance*.

If organizations are to realize maximum value from IT investments, they must first take steps to prevent or mitigate the impact of any disaster. Therefore, effective IT Risk Governance—the minimum level of IT governance a firm should enact—should precede any attempt at IT Value Governance. The remainder of this article deals exclusively with IT Risk Governance.

**A Contingency Model of IT Risk Governance**

The amount of time and Board attention spent on IT governance should be a function of the IT intensity of the firm. Organizations with comparatively little investment in information technology would necessarily spend less time and resources on IT risk governance than information-intensive organizations such as banks. Nolan and McFarlan capture this notion in the IT Strategic Grid
framework, illustrated in Figure 1. It advises executives to assess the relative importance of their current information technology, on a continuum ranging from low-to-high, and the strategic value of future investments in IT. Firms in a high-high situation (i.e., IT is critical currently and will continue to be so in the future) are the most IT-intensive, while those in the low-low situation are the least.

The greater the relative importance of IT to the firm’s ongoing operations, or the closer an organization is to the high-high situation, the greater the risk. For example, banks have large capital investments and would be crippled without the ability to record deposits, dispense cash, reconcile accounts, and process credit-card charges electronically. Their future products are also dependent on IT. On the other hand, while very few firms are not dependent on IT for at least back-office processing, for some organizations, IT investments are relatively unimportant. For example, a traditional university, while it would be inconvenienced by a system outage, would not be crippled, for the organization’s value resides primarily in the intellect of faculty not on using information technology. In this case, IT plays a support role, maintaining student records, class schedules, and financial information. While we are not suggesting that the university could operate for a long time without its information systems, its core activities—research and teaching, could continue.

**The IT Risk Governance Chain**

The metaphor of a “chain” has a strong tradition in the management literature. The value chain, introduced by Porter and Millar in the 1980s, suggested
that an organization can be viewed as a set of interconnected primary and secondary activities, each adding value.

The notion of a value chain for IT Governance implies that managing IT risk consists of a series of linked actions by actors within and outside of the organization, with the whole chain only as strong as its weakest link. It suggests that IT risk management is an iterative and ongoing undertaking by Boards and their agents. Finally, it assumes that crises averted and losses minimized all create value for the firm by not squandering its assets (time, money, and people). The Risk Governance Chain has two parts.

The first part of the chain (Figure 2A) shows the relationship between the Board and management with respect to IT investments. It illustrates that the Board is ultimately responsible for managing IT-based risk, and it cannot continue to be, as Huff et al. suggest, its weakest link. The Board elects an Audit Committee composed of outside directors, responsible for monitoring financial reporting and enterprise risk. This committee receives reports from the organization’s internal auditors, who focus mostly on process efficiency and compliance (in the case of regulated industries) as well as enterprise risk, and from the external auditors appointed by the company’s shareholders, who focus on complete and accurate financial reporting. As the organization’s information systems are chiefly the means by which transactions and financial performance is recorded, the organization’s Chief Information Officer (CIO) often reports to the Board and Audit Committee on process integrity.

Ideally, the audit committee triangulates input about IT: the organization’s Chief Information Officer (CIO), the external auditors, and internal auditors. If the CIO is relied on exclusively as a key informant, this is tantamount to a Board telling the CFO: “No need for financial statements—we trust you when you say that the organization is financially sound.” Paul Strassman, who has argued for years that companies need to understand IT value the way CFOs understand financial value, said, “My hope is for the CIO of the future to be eligible to go to jail.” His point in saying this is that CFOs control only about one third of an organization’s assets—the financial ones. The remaining two thirds of the assets are based on intellect, much of which is captured, stored, and used in decision making through use of information systems and technology. Some economists assert that the breaches of trust (e.g., at Enron, ImClone, WorldCom, and Global Crossing) that resulted in passage of the Sarbannes-Oxley Act (SOX) were all crimes of information partly involving an unsupervised expert. While Boards will continue to rely on experts such as the CIO for advice, the responsibility remains theirs. The value chain affirms the importance of the CIO, but lets her know that the Board will be exercising oversight by consulting a number of sources, looking for convergence and consistency.

**IT Risk and IT Governance**

There are many IT Governance frameworks that have been compiled by various international standards bodies to assist the provision of IT services.
These frameworks (see Appendix 2 for a list of the most prevalent) represent the best examples of conventional wisdom regarding IT management for CIOs, IT managers, and other executives in the organization. Many senior IT managers use principles and processes from these frameworks to effectively manage the investment, deployment, and operational support of IT. However, none of them are at the Board level, nor do they address directors’ duties and responsibilities. Another issue is that if they relate directly to IT Governance, like the work of Weill and Ross, they deal almost exclusively with IT value creation rather than risk avoidance.

From the perspective of Boards, these frameworks are either too simplistic and high-level or too detailed and technically focused to be implemented by Boards. Recognizing the complexity of IT, the U.S. Securities and Exchange Commission (SEC)—on May 17, 2006, and again on August 9, 2006—offered listed companies relief from SOX section 404 compliance, including a slower pace of compliance inspection, reduced auditing verification, and guidelines clarifying compliance requirements.

Our analysis of these frameworks suggests that there are three primary targets of IT risk management—the security of data and information, the integrity of hardware and systems, and the implementation of IT projects. Risk management requires plans and procedures for each IT target. These areas cover, albeit in a different form, the key IT resources identified by Guldentops: data, application systems, technology, facilities, and people.

By combining findings from our case studies and common elements from the global standards, we have developed a typology of IT Risk that can be governed at the Board level. There are five interrelated categories of risk:
IT Competence Risk, Infrastructure Risk, IT Project Risk, Business Continuity Risk, and Information Risk.

To complete the IT Governance Chain, we now include these five categories of risk in the full model, shown in Figure 2B. By monitoring these five categories of IT-based risk using the Director’s Dashboard, Boards can discharge their IT risk governance responsibilities.

**A Director’s Dashboard for IT Risk Governance**

We do not suggest that directors spend all their time on IT governance. However, evidence suggests that most Boards need to spend more time than they have in the past. Time is the scarcest resource for Boards, and directors must rely on principles, frameworks, and external resources to discharge their duties.

The dashboard is structured around a set of questions for each area of risk. This approach was suggested by Guldentops “While it is not the most efficient IT Governance process, asking tough questions is an effective way to get started. Of course, those responsible for governance want good answers to these questions. Then they want action. Then they need follow-up.”

Each of the five elements in this dashboard consists of two key questions for which directors need to find an answer. The dashboard then provides three guidelines to assess the answers received: Red (an unacceptable level of risk that needs to be addressed immediately); Amber (cautionary risk suggesting that one or two critical aspects of the factor have not been adequately addressed); and Green (no undue risk exists and/or all risks have been mitigated).
If Boards implement this framework, they will use their time efficiently and effectively, discharge their fiduciary responsibilities towards safeguarding investments in the information assets of the organization, and provide meaningful feedback and direction to management. As noted above, this is the minimum effort required to govern IT Risk. Boards with advanced expertise or very high risk in a specific area will develop more nuanced processes.

**IT Competence Risk**

This risk factor refers to the IT knowledge of directors. The more directors know about IT, the more they can understand its impact on the firm’s strategy and its risk profile. The basic problem currently is that most directors did not achieve their prominence in the business community by understanding and managing IT. Those that did must re-train due to the short half-life of their knowledge. Gonzalez describes this challenge: “Technology is placing unique requirements on people in the workplace…compelling a sharp focus on training and education…Half of what is known today was not known 10 years ago.”

The rate of technological change and its complexity means that whatever knowledge one has about IT will be obsolete within two to five years.

Firms with a high level of IT intensity must have IT competence available within the Board. In general, directors need to acquire and maintain adequate knowledge of information technology if they are to responsibly discharge their duties with respect to its governance. In addition, Boards may need to identify a Lead Director for information technology who will take a leadership role in bringing IT issues to the Board’s attention—the same way that many Boards have a Lead Director for accounting, investment, or legal matters. If no such Director is currently appointed, then the Board needs to recruit for these specific skills.

Figure 3 represents the first element of the dashboard.

**Infrastructure Risk**

The IT infrastructure refers to the digital undercarriage of the organization—the computers, networks, operating systems, applications, and databases.
that provide the firm with its IT assets. There are two major elements of Infrastructure risk—the first being internal risk created by failure of systems, technologies, or networks. This area of risk is usually well understood in organizations since it has been the focus of IT management attention for decades.

The second is the external risk that has arisen since organizations became connected to the Internet. These risks come from sources such as hackers, viruses, worms, and spam. Intrusions from these outside agents can cripple an organization, making it impossible to deliver services to customers, suppliers, and employees. If the organization’s defenses are breached, the risk moves into the organization and can attack critical systems and information.

Threats from external sources are increasing. For example, Postini, a leader in enterprise spam-blocking software, reported that in December 2006, spam accounted for 93 percent of all electronic mail on the Internet. This represents a 144 percent increase from December 2005. More recently, on February 5, 2007, three of the Internet’s 13 “root” servers (those controlling traffic to the “.org” and “.uk” web sites) came under overwhelming attack from zombie computers, temporarily disrupting traffic to these web sites and slowing the entire Internet down considerably. As a result of these and other risks, every year a larger percentage of IT budgets is spent on risk prevention.

A second source of external risk comes from IT partners such as vendors and contractors. The growing trend to offshore data processing, help-desk support, training, and implementation has loosened the organization’s control over its core IT activities. The extent to which the Board is aware of the scope of offshoring and outsourcing, and the mechanisms that have been put into place to manage and control these contracts, reflects the salience of this risk to the organization.

In order to manage this risk, one firm we studied provides its directors with an IT governance worksheet that divides infrastructure risk into five broad categories—Business Application Needs, IT Investments & Prioritization, IT Principles, IT Infrastructure Strategies, and IT Architecture. Each of these areas is assigned a senior manager sponsor that liaises with directors on the Board’s audit and/or executive committees. In this way, the company articulates the risks and then quantifies and prioritizes them. At Board meetings, the committees’ conclusions are presented and discussed.

Figure 4 represents the second element of the dashboard

*IT Project Risk*

Sauer, Gemino, and Reich have recently completed a study of IT project performance, concluding that project size, complexity, and management practices in the organization dramatically affect IT project success rates. This risk category captures the risk inherent in new and typically large IT initiatives.

IT projects, particularly those that are changing the core processes of the organization, have the ability to completely destabilize operations and put them at risk. As highlighted in the financial implications of the project disasters noted at the beginning of this article, writing off these debacles assumes that
companies survive. Our research has shown that this is not always the case. For example, Rich Con Steel, a 143-year-old business in Kansas City, shut its doors in 1999 after a disastrous IT implementation. The failure of Sobeys ERP implementation was severe but not fatal. The system shut down for five days and employees were left scrambling to stock empty shelves and pay suppliers for weeks.

Organizations that rely on IT projects to improve and transform their operations must invest in developing IT Project competence. From a director’s perspective, the existence of a corporate Project Office, certification for project managers, and the adoption of a portfolio mindset for selection and monitoring of key projects are indicators that the organization is committed to increasing its project competence.

Figure 5 represents the third element of the dashboard.

**Business Continuity Risk**

Post 9/11, most organizations put emergency measures in place. For example, the Chief Information Officers (CIOs) of Merrill Lynch, Deutsche Bank, Lehman Brothers, and American Express—all major tenants of the World Trade Centre—spent the better part of the remainder of 2001 and 2002 decentralizing their operations and striving to minimize the effects of future terrorist attacks or natural disasters. This included physical separation of data processing centers, logical separation of duties, offsite data storage and recovery, and preparation of a comprehensive business continuity plan.

However, this risk category refers to more than just plans for internal company operations. It also considers underlying societal infrastructures. For example, one company we studied decided not to offshore part of its data processing because of that country’s communications infrastructure. The company felt that it could not afford to lose either track or control of its data if a widespread network failure occurred (as was the case recently, when power blackouts affected the region).
This risk category refers to an organization’s internal weaknesses, susceptibility to external disasters and the stability of environmental factors (e.g., political and/or social infrastructure stability in a developing nation). As such, it is incumbent on Directors to reassure themselves that not only has a comprehensive continuity plan addressing all of these areas been prepared, but that this plan has been tested and found to be robust.

Figure 6 represents the fourth element of the dashboard.

**Information Risk**

The advent of data loss, privacy laws, and anti-spamming legislation have created an imperative for organizations to: collect only those data it absolutely needs for business purposes; use these data only in the manner authorized; and safeguard the data from intrusion, unauthorized use, or inappropriate modification. Failure to do so may at the very least lead to embarrassing publicity and, at its worst, to legal action (as in the case of the aforementioned TJX Cos., where
a pending lawsuit may imply that stakeholders are linking fraud with negligent IT risk management). Last year, ChoicePoint settled with the Federal Trade Commission (FTC) for $10 million in civil penalties and $5 million for consumer redress as a result of the security breach that saw over 150,000 consumer records stolen. Ameritrade agreed to pay the Massachusetts State Regulator $25,000 to cover costs incurred for investigating the theft of one employee’s laptop computer that contained customer names and social security numbers. The Privacy Rights Clearinghouse, which began tracking security breaches after the February 15, 2005 breach at ChoicePoint, reports that over 100 million records containing sensitive personal information have been involved in 474 security breaches worldwide—108 such breaches in 2005, 331 breaches in 2006, and 35 breaches in the first 34 days of 2007.

Boards need to satisfy themselves that appropriate privacy policies are in place, that these policies conform to laws in their place(s) of incorporation, and that, most importantly, a privacy officer has been named and possesses sufficient time, knowledge, and authority to enforce these policies aimed at preventing breaches or their catastrophic consequences.

Figure 7 represents the fifth and final element of the dashboard.

**Conclusion**

Whatever mode it takes—centralized or decentralized, staff-led or board-led—IT Governance must be actively embraced by the Board if the organization is to be responsible to its stakeholders. About two-thirds of all capital spending is devoted to information technology, and around 40% of that comes to the Board for approval. This exploratory research affirms earlier work that holds directors should spend greater time and attention on IT issues, and it suggests a minimum number of areas that should be considered by directors.

For too long, the absence of IT crises has led some Boards into complacency. They have relegated their IT governance responsibilities to CIOs. These
CIOs have, for the most part, acquitted themselves well. However, today’s regulatory climate, external risks from criminals, and the growing scope and complexity of IT projects make a compelling case for strong IT governance to be a priority for the Board. Good IT governance is an effective means to reduce risk, mitigate the impact of IT-related disasters, lower the cost of capital, and create enduring shareholder value. The IT Risk Governance Chain and the Director’s Dashboard presented here can provide the foundation for Boards as they govern IT risk.

APPENDIX 1
Firms Participating in this Study

<table>
<thead>
<tr>
<th>Firm</th>
<th>Industry / Country</th>
<th>Size</th>
<th>Size of Board</th>
<th>Size of Audit Committee</th>
<th># Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Financial Services (Australia)</td>
<td>Small</td>
<td>9</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>B</td>
<td>Logistics (Canada)</td>
<td>Medium</td>
<td>13</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>Financial Services (Canada)</td>
<td>Large</td>
<td>17</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>Healthcare Administration (U.S. &amp; Canada)</td>
<td>Large</td>
<td>14</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>Retail (Canada)</td>
<td>Medium</td>
<td>9</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>Data Processing &amp; Warehousing (U.S.)</td>
<td>Medium</td>
<td>11</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

APPENDIX 2
IT Governance Frameworks

<table>
<thead>
<tr>
<th>Framework</th>
<th>Origin / Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoBIT</td>
<td>Control Objectives for Information and related Technologies—developed by the IT Governance Institute (ITGI—&lt;www.itgi.org&gt;) for the Information Systems Audit and Control Association (ISACA—&lt;www.isaca.org&gt;)</td>
<td>First published in 1996, and now in its fourth version, this is a best practices framework that lists 34 high-level objectives covering 215 control objectives grouped into 4 domains: Plan and Organize; Acquire and Implement; Deliver &amp; Support; and Monitor and Evaluate.</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organizations of the Treadway Commission—&lt;www.coso.org&gt;</td>
<td>A private-sector initiative formed in 1985 to deal with fraudulent financial reporting. Published its 8-component Enterprise Risk Management Integrated Framework in 2004 as a result of the passage of SOX in 2002. This framework has been endorsed by the SEC as SOX-compliant.</td>
</tr>
<tr>
<td>Framework</td>
<td>Origin / Definition</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ITGDF / GAM</td>
<td>IT Governance Design Framework / Governance Arrangements Matrix—P. Weill and J. Ross, IT Governance (Cambridge, MA: Harvard Business School Press, 2004)</td>
<td>Part of the ITGAP process, in which managers first map IT-related processes in their organizations before changing them to conform to one or more governance archetype.</td>
</tr>
<tr>
<td>CMM / CMMI</td>
<td>Capability Maturity Model / Capability Maturity Model Integration—Software Engineering Institute at Carnegie-Mellon University (&lt;www.sei.cmu.edu/cmmi/&gt;)</td>
<td>CMM was originally developed in the mid-1980s to aid in managing large software development projects. It posits 5 maturity levels. CMM was replaced by CMMI, which is broader in scope to include most business processes.</td>
</tr>
<tr>
<td>IT Service CMM</td>
<td>Information Technology Service CMM (Consortium of 3 companies and 3 universities in the Netherlands, c1998—the Kwintes Project (&lt;www.itservicecmm.org&gt;))</td>
<td>Capability Maturity Model for providers of IT services, with corresponding levels of service maturity.</td>
</tr>
<tr>
<td>ITIL V3</td>
<td>IT Infrastructure Library—(&lt;www.itil-itsm-world.com/&gt; or &lt;www.itil.co.uk&gt;)</td>
<td>ITIL is a guiding framework of best practices for service and asset management. In its 3rd version, it currently consists of 5 best practice volumes focused around the service lifecycle and continuous service improvement.</td>
</tr>
<tr>
<td>ASL</td>
<td>Application Services Library—(<a href="http://www.aslfoundation.org">www.aslfoundation.org</a>)</td>
<td>Provides a framework for IT applications development that centers on 3 areas: functional management, application management, and technical management.</td>
</tr>
<tr>
<td>SDM / SDM2</td>
<td>Software Design and Management—(Cap Gemini, <a href="http://www.capgemini.com">www.capgemini.com</a>)</td>
<td>Developed in 1970 (by Pandata—since bought by Cap Gemini) and revised in 1987, it presents a 7-stage waterfall model.</td>
</tr>
<tr>
<td>SAS 70</td>
<td>Statement on Auditing Standards no. 70—American Institute of Certified Public Accountants (AICPA) &lt;www.sas70.com&gt;</td>
<td>Developed in 1992 as a follow-on to SAS 55 (internal controls), this is an auditing standard to assess the internal controls on transaction processing. Became the basis of the standard eventually advocated by COSO.</td>
</tr>
</tbody>
</table>

**Framework**

IT GAM:


- **Description**: A set of 5 IT Decision Domains (principles, architecture, infrastructure, business applications, investment). Weill and Ross show how to govern each domain for optimal value creation.

ITGDF / GAM:


- **Description**: Part of the ITGAP process, in which managers first map IT-related processes in their organizations before changing them to conform to one or more governance archetype.

CMM / CMMI:

- **Origin / Definition**: Capability Maturity Model / Capability Maturity Model Integration—Software Engineering Institute at Carnegie-Mellon University (<www.sei.cmu.edu/cmmi/>)

- **Description**: CMM was originally developed in the mid-1980s to aid in managing large software development projects. It posits 5 maturity levels. CMM was replaced by CMMI, which is broader in scope to include most business processes.

IT Service CMM:

- **Origin / Definition**: Information Technology Service CMM (Consortium of 3 companies and 3 universities in the Netherlands, c1998—the Kwintes Project (<www.itservicecmm.org>))

- **Description**: Capability Maturity Model for providers of IT services, with corresponding levels of service maturity.

ITIL V3:

- **Origin / Definition**: IT Infrastructure Library—(<www.itil-itsm-world.com/> or <www.itil.co.uk>)

- **Description**: ITIL is a guiding framework of best practices for service and asset management. In its 3rd version, it currently consists of 5 best practice volumes focused around the service lifecycle and continuous service improvement.

ASL:

- **Origin / Definition**: Application Services Library—(www.aslfoundation.org)

- **Description**: Provides a framework for IT applications development that centers on 3 areas: functional management, application management, and technical management.

SDM / SDM2:


- **Description**: Developed in 1970 (by Pandata—since bought by Cap Gemini) and revised in 1987, it presents a 7-stage waterfall model.

SAS 70:

- **Origin / Definition**: Statement on Auditing Standards no. 70—American Institute of Certified Public Accountants (AICPA) <www.sas70.com>

- **Description**: Developed in 1992 as a follow-on to SAS 55 (internal controls), this is an auditing standard to assess the internal controls on transaction processing. Became the basis of the standard eventually advocated by COSO.

ISO/IEC 20000:


- **Description**: Specifications and Code of Practice for IT Service Management. It is the first international standard for IT service management and is aligned with ITIL best practices.
Notes

1. We use “Information Technology” or “IT” in its broadest context, that is, the sum of all hardware, software, policies, procedures, data, and people that work together in creating and managing the information resources of an organization.


22. S.L. Huff, P.M. Maher, and M.C. Munro, “Information Technology and the Board of Directors: Is There an IT Attention Deficit?” *MIS Quarterly Executive*, 5/2 (June 2006).
34. Huff et al. (2004), op. cit.
38. U.S. Securities and Exchange Commission Press Release 2006-136, “SEC Offers Further Relief From Section 404 Compliance For Smaller Public Companies And Many Foreign Pri-
45. Interview with Martha Sawyer, then-President of Rich Con Steel, by the first author, November 11, 2003.
48. CIO Staff, op. cit.
50. Ibid.