

- [Magazine](#)
- [Subscribe](#)
- [Events](#)
- [Tech Jobs](#)
- [Backlog](#)
- [About](#)
- [News Releases](#)
- [Media Kit](#)
- [Supplements](#)
- [Books](#)
- [Site Search](#)
- [GO!](#)

- [Top 300 - 2009](#)
- [Latest Issue](#)
- [Archive](#)
- [Editor's Letter](#)
- [From the Publisher](#)
- [Jim Harris](#)
- [Sponsors / Advertisers](#)

**Current Issue**



**Tech and Business Videos**



**Portals**

[Backbone's categories](#)

[Careers](#)

[Data Management](#)

[Economic Development](#)

[Education](#)

[Green](#)

[Health](#)

[Olympic Tech](#)

[Outsourcing](#)

[Security](#)

[Social Networking](#)

[Tech Associations Canada](#)

[Travel](#)

[Unified Communications & VoIP](#)

[Web 2.0 PICK 20 Winners 2009](#)

[Wireless](#)

**Understanding governance**

May 5, 2008

**IT governance is a complex beast. We take you through some of the legislation, standards and best practices**

By [Danny Bradbury](#)



You run a bank and you are in a quandary. A new technology is emerging that will change the way customers interact with you; in the '70s it may have been ATM cards, now perhaps it's contactless payments, but in any case all the banks want to be first on the scene with this feature. It is expected to make life more convenient for customers and lower your business costs. There are risks involved with deploying the technology, though. The project may come in over budget, take too long to implement, or the technology may be susceptible to fraud. How can you quantify those risks? Plus, these aren't the only risks you must assess. There are dangers inherent in not implementing the technology, including the possibility of losing customers to other banks and finding your competitors can do business without investing as much money. Your board of directors must weigh the technical and business risks carefully and make a decision, but it can only do that properly if the necessary intelligence is available from the computing department. Welcome to the world of IT governance, and specifically, to the intersection of IT and corporate governance.

When most people think of governance, compliance probably springs to mind. Enron's bankruptcy in 2001 following runaway fraud led to the creation of the Sarbanes-Oxley Act (SOX) the following year, which sought to impose tighter controls on the way companies operated. Canada's milder SOX equivalent, Bill 198, came into effect a year later. Other controls such as the banking industry's BASEL II and the industry-imposed PCI-DSS rules for handling credit card data have also led companies to question how well their IT departments are protecting their systems and information.

Recent events have highlighted the relationship between risk management in the IT department and the broader business world more than ever. Michael Parent, director of the CIBC Centre for Corporate Governance and Risk Management at Simon Fraser University's Segal Graduate School of Business, highlights the TJX debacle, in which the retail group lost tens of millions of customer records to thieves following a lapse in IT security.

"TJX's share price took a 3.5 per cent drop two days after the class-action lawsuit was filed," he said, also recalling the Federal Trade Commission's investigation of the group six weeks later. "That opens you up to shareholder lawsuits."

**Help available**

Best-practice guidelines, which can help manage risk and avoid these types of problems, are relatively well documented. "When people want to implement IT governance and they rely on the proper framework, it's much easier and goes much more efficiently," said Michael Lambert, an associate professor who teaches IT governance at Sherbrooke University in Quebec.

Several standards focus on particular aspects of IT governance. For example, ISO 27001 and 27002 set out specific security practices for applications in an IT context, which is a focal point for much compliance-driven governance activity. But with high-profile data breaches regularly covered by the press, it is easy to forget that IT is about more than locking down computer security. Simply throwing a best-practice security document at a computer team and following up six months later with an audit won't cut it.

Lambert refers instead to a definition of governance issued 10 years prior to SOX. The U.K.'s 1992 Cadbury Report on the financial aspects of corporate governance has become a template for many institutions.

"Corporate governance is the system by which companies are directed and controlled," the report said. This direction goes beyond simply covering your corporate behind against security threats. It includes setting strategic goals, supervising the management of the business and reporting on the leaders' stewardship.

Frameworks that address this broader view of governance run into double figures. Among them are the Information Technology Infrastructure Library (ITIL), published by the U.K. government, which is a set of best practices for providing IT services to end users.

Others include AS 8015, an Australian methodology that has been adopted internationally, and IT GAM, a matrix of different areas of IT developed by Peter Weill and Jeanne Ross, two professionals lauded for their approach to IT governance. In North America, the Control Objectives for Information and related Technology (COBIT) lays out best practices for running an IT department.

"It's all summed up in the five fundamental dimensions of IT governance," Lambert said, describing

Look Sharp and Work Smart  
**SCAN IT NOW**  
ScanSnap S1500

**FUJITSU**

Top Lists and Tech Tips

[more Top Lists and Tech Tips](#)

Yahoo! Search Marketing \$100 credit

Find your **Online Marketing Target Audience**

**YAHOO!** SEARCH MARKETING

**Enhanced Targeting**  
\$100 credit for Backbone readers

Gadget of the Week

Samsung 2233RZ 3D monitor  
[more Tech Gadgets](#)

COBIT.

- Strategic alignment ties together business and IT plans so that the computing department works toward the goals that the board has laid out.
- Value delivery makes sure that IT delivers the benefits that were promised.
- Resource management concerns the management of applications, information, infrastructure and people within the computing department.
- Risk management reflects organizational tolerances for risk in IT operations.
- Performance measurement enables the board to understand how well the computing department is executing its tasks.

These five struts of IT governance don't exist independently, however, picking one without addressing the others is difficult. For example, change management procedures (such as applying new system patches) may be considered a resource management issue, but also affect the level of risk within the organization because the frequency and speed of system patches or other changes could affect your vulnerability to security exploits.

#### Assessing compliance

For a truly holistic approach to IT governance, however, Tony Balasubramanian, a partner in advisory services at PricewaterhouseCoopers (PwC) Canada, suggests that even the broadest governance frameworks such as COBIT must be complemented by other elements. He envisages three layers of IT governance, with best-practice frameworks constituting the filling in the pie.

Above those frameworks lie the strategic IT decisions that must be made to support the business, he explains. "At the bottom layer, you have the things that support those COBIT and ITIL frameworks. They're things like job descriptions, skills and competency development in IT, and management of employees so that you can get them up to a sufficient competency level."

Unfortunately, employee training is the biggest challenge facing small (sub-1,000 employee) companies considering governance strategies, according to IDC. Lambert also emphasizes the importance of producing IT governance skills in academic institutions, and said that there are too few courses focusing on this. Perhaps that's one reason why most of the experts Backbone interviewed believe Canada isn't governing its IT very well.

"You'd have to question how far along the Canadian marketplace is in asserting that IT is in a good state to be able to do those things," said David Senf, IDC Canada's director of security and software research.

"The situation in Canada is significantly different from the U.S. in that we have way more smaller-sized companies," said John Singleton, former auditor general for Manitoba, and a former president at the Information Systems Audit and Control Association (ISACA), which co-developed COBIT. He argues that, generally, these companies aren't driven to comply with SOX, which has been a big driver for governance initiatives in larger firms.

However, Senf said that even larger companies are experiencing limited success. "In organizations with over a thousand employees, we see a better penetration of standard best practice for governing IT," he said. "But where they are adopted, we don't see that many IT organizations are far along with that."

#### Grim IT picture

If we're falling down on IT governance, who's to blame? No one is manning the rudder, Senf said. "You ask [IT departments] why they're not doing more, and invariably they point to management and say 'there's not the proper leadership in our organization to push us to do this, or to put the proper budgets or policies in place to allow the organization to do more.'"

Singleton points to a fundamental cultural divide between IT professionals and businesses. The fault there lies with the board, said SFU's Parent. In a study evaluating the presence of IT expertise on the board, he found Canada ranking a sorry fourth behind Britain, Australia and the U.S. (and the state of those countries wasn't much better).

"It's a pretty grim picture," he said. "It's one of these things that we all know we need to do, but we don't do it until a crisis occurs, and then we get religion."

Therein lies the problem. Senior management has traditionally viewed IT as a black box; a mysterious discipline in which obscure technical things happen, and into which money flows and the occasional productive system flows out. And yet in an age where the fortunes of many companies are intrinsically tied to the quality of their computing operations, having a solid understanding of IT on the board amounts to a fiduciary duty, Parent said; it's table stakes.

"Boards are being negligent in discharging their responsibilities in terms of IT in the organization from two perspectives," he warns. Firstly, they're not minimizing the risks associated with IT investments, but they're also failing to acknowledge the successes that investments in IT can bring.

He proposes a structured model for communicating risk to senior management. There are five broad types of IT risk, he said: competence, infrastructure, project risk, business continuity and information risk. These should be subject to both internal and external audit, he said, and the audit committee responsible for that should report to the board.

What about fulfilling the board's other duty: to properly align IT with business strategies in an accountable way, ensuring that it is used effectively to drive new efficiencies into the business? "At the board level, it's about going beyond the compliance and control issues with technology, and seeing the value of it," said Nicole Haggerty, assistant professor of management information systems at the Richard Ivey School of Business. "They need to shape a framework of accountability. Who makes decisions? Who gets involved in them, and what are the core decisions that need to be made around business priorities and architecture?"

This requires regular meetings between the board and IT, said PwC's Balasubramanian. Other methodologies may be useful here. Another framework from ISACA, called VALIT, is based on COBIT but extends it to connect IT with the board's strategic objectives.

#### Getting started

We may now understand what IT governance means, but embarking on such an initiative will be a daunting task for many companies. How can it be done? Many will choose to focus on the risk management aspect as a crucial factor and leave the other elements of governance for the time being.

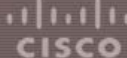
"Operations and efficient service organization are two very important things but given our size they haven't been issues," said Neil Beaton, CIO at Pacific & Western Bank of Canada, which runs its systems entirely on PC technology and maintains just 60 staff. Instead, his main focus is on formalizing risk management, he said. "We don't have the same formal infrastructure adoption challenges that a large corporation would have."

No matter how scaled back your IT governance operation, you'll still need money to make it work, said Carmi Levy, a former CIO in the finance sector and Info-Tech research analyst, and now senior vice-president in strategic consulting at technology advisory firm AR Communications. "You have to have budgetary approval in the first place," he said.

It isn't surprising that risk management sits at the top of most companies' radar when it comes to IT and corporate governance. No wonder people like Beaton are starting there. But Levy is one of many who insist that this is just the tip of the iceberg.

Once IT departments have convinced the board of the need for effective IT risk management, they should be advocating a stronger emphasis on the other aspects of governance that could cement the relationship between the server room and the boardroom. "You have to show how much this ad hoc approach to service delivery is costing," Levy said, and then follow up by explaining how beneficial a formalized, strategic link between IT and the board can be.

[ExecutiveOverview Archive](#)



[Magazine](#) | [Events](#) | [Careers](#) | [Backlog](#) | [Press Release](#) | [Book Review](#) | [About Us](#) | [Media Kit](#)

© 2006-2007 Backbone Magazine. All Rights Reserved. [Privacy Policy](#) | [Terms of Use](#).