

Taming Information Technology Risk

A New Framework for Boards of Directors

OLIVER WYMAN



Published by:
National Association of Corporate Directors®

© Copyright 2011.
National Association of Corporate Directors
Two Lafayette Centre
1133 21st Street NW, Suite 700
Washington, DC 20036
202-775-0509
www.NACDonline.org

Permission is hereby granted to print this document with the following citation: “Reprinted with the permission of the National Association of Corporate Directors.” © 2011 National Association of Corporate Directors. Reference: NACD White Paper: *Taming Information Technology Risk: A New Framework for Boards of Directors.*” All other rights reserved.

Managing Director, Peter R. Gleason
Chief Knowledge Officer, Dr. Alexandra R. Lajoux
Research Manager, Kurt L. Groeninger, Esq.
Research Analyst, Katherine Iannelli
Editor, Suzanne L. Meyer

Special thanks to the authors:

Jonathan Cohn, Partner, Financial Services, Oliver Wyman

Jonathan Cohn is a partner within Oliver Wyman’s Strategic IT & Operations Practice, focused on working with senior business and IT executives on critical growth, cost, risk management, and regulatory transformation initiatives. He has over 18 years of diverse strategy consulting, technology, and operations experience, and has provided expert guidance on board-level IT risk issues and data strategy and governance. Prior to joining Oliver Wyman, Mr. Cohn was a founding member and associate partner within IBM’s Financial Markets IT Strategy & Transformation Practice.

Mark Robson, Partner, Global Risk & Trading, Oliver Wyman

Mark Robson is a partner at Oliver Wyman. He has over 20 years experience in developing leading edge approaches to valuing assets with drivers linked to hard-to-quantify contingencies. He specializes in designing tools enabling clients to conduct risk adjusted strategic planning, capital budgeting, portfolio modeling, commodity hedging and mitigation optimization. His experience spans airlines, insurance companies, energy, chemical, technology companies and international financial institutions.

Table of Contents

About the National Association of Corporate Directors	4
Taming Information Technology Risk	5
The IT Governance Dilemma.....	5
A New Framework	6

ABOUT NACD

The National Association of Corporate Director's (NACD) mission is to advance exemplary board leadership—for directors, by directors. We deliver the knowledge and insight that board members need to confidently navigate complex business challenges and enhance shareowner value. We amplify the collective voice of directors in setting a substantive policy agenda.

The Association was founded in 1977 as the only national membership organization created by and for directors. Today, 11,000 directors and key executives from public, private, and nonprofit companies rely on us for board development, education, and connections.

NACD's Leading the Way initiative provides essential resources that help directors strengthen board leadership. The *NACD Key Agreed Principles* document a consensus among directors, executives, and shareowners on benchmarks for leading practices. Through initiatives such as these, NACD empowers directors to anticipate, influence, and meet boardroom challenges while effectively leading their organizations. For more information or to join NACD, please visit www.NACDonline.org or call 202-775-0509.

About Oliver Wyman

With offices in 50+ cities across 25 countries, Oliver Wyman is an international management consulting firm that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, organizational transformation, and leadership development. The firm's 3,000 professionals help clients optimize their businesses, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is part of Marsh & McLennan Companies [NYSE: MMC]. For more information, visit www.oliverwyman.com.

Taming Information Technology (IT) Risk

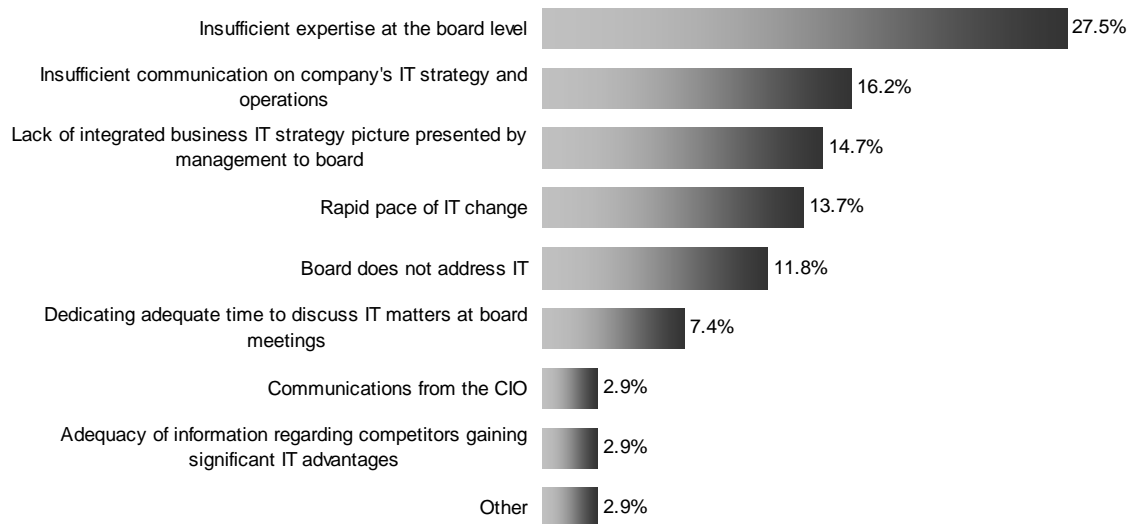
It used to be clear which firms were technology businesses. They were core providers of technology itself (IBM, Microsoft, Apple) or later, the leaders in the new technology-centric Internet culture (Google, eBay, Amazon, Yahoo). But today, every business is a technology business. No matter what industry, companies rely on technology to squeeze costs, streamline processes, leapfrog competitors, and, where possible, transform whole industries. Yet while some management teams have kept pace with rapidly changing technologies to succeed in today's business environment, it is the very rare board that has been able to provide the governance and leadership that is so desperately needed in this area.

A recent survey of 204 board members by Oliver Wyman's Global Risk Center and the National Association of Corporate Directors (NACD) finds that nearly half (47%) of board members are dissatisfied with their board's ability to provide IT risk oversight. When you consider how much is riding on companies' ability to use technology effectively, that figure is alarming. The world's largest 500 companies lose more than \$14 billion every year because of failed IT projects, according to an Oliver Wyman analysis. Therein lies an opportunity. Companies that receive valuable board direction and input on IT-related risk will have a significant competitive advantage over those that don't.

The IT Governance Dilemma

The pace of technological change is continually accelerating: Think how different the technology landscape looked just ten years ago. In 2001, there were no iPhones delivering "apps" on the go, social media was in its infancy, and few people had heard of

Stumbling Blocks for Boards



Source: NACD/Oliver Wyman, 2010

cloud computing. Keeping up with these advances and dealing with the threats and opportunities they create is extremely difficult for IT professionals, never mind for “lay people.”

It’s unfortunate, then, that fully half (51%) of those board members surveyed say they aren’t given enough information to perform their IT oversight duties. Few board members have extensive IT experience: Only 16% of survey participants report having been a CIO or senior IT executive earlier in their career.

While opinions differ on the degree of importance IT will have on the future of the companies they govern, there is near unanimous agreement that it will markedly change the company’s performance. More than 99% of survey participants believe that IT will have a significant impact on the organization in the next five years. More than one-third (36%) expect IT to improve operational efficiencies, while 30% believe IT will provide a competitive advantage for their company in the next five years. Nineteen percent harbor even higher expectations: They believe IT will transform their company.

A Framework for IT Risk

<p><u>Competitive Risk:</u></p> <p>The threat of competitors getting to market faster, gaining market share, or achieving an insurmountable first-mover advantage through the use of technology.</p>	<p><u>Portfolio Risk:</u></p> <p>The danger that a corporation is spending too much of its scarce IT dollars and resources on basic operational expenses instead of truly transformational investments.</p>
<p><u>Execution Risk:</u></p> <p>The failure to execute IT programs effectively or to deliver critical capabilities to the business on time and on budget.</p>	<p><u>Service & Security Risk:</u></p> <p>The risk that systems aren’t available to support and/or service employees and customers as needed and that critical data assets of the firm are not properly secured.</p>

What’s more, the vast majority of board members surveyed say that oversight of IT risk *should* be the board’s responsibility. Boards want to provide counsel and direction, and shareholders and senior management expect them to do so—especially on the most challenging issues that impact the future of the corporation. Clearly, then, what boards urgently need is a different way to approach the breadth of IT-related issues.

A New Framework

Given the many areas of a business that IT touches, IT risk shouldn’t be viewed as a monolithic issue. Rather, boards should consider IT in the context of a wide range of business concerns. Our framework, consisting of four pillars of risk, will give boards and executives a common language to address IT-related risks. The four areas of risk the firm could be exposed to by ineffective management of IT are: *competitive, portfolio,*

execution, and service and security. Below is an examination of each of these risks in turn.

1. Competitive Risk: Threats here include the risk of competitors getting to market faster, gaining market share, or achieving an insurmountable first-mover advantage. That may happen through the introduction of a new technology that changes the channel to the end-consumer, dramatically alters the pricing or economics of a given business, or eliminates the need for the company's products and services.

One well-known example is the iPod. Apple wasn't the first company to introduce an mp3 player. It was the first one to revolutionize the way customers legally bought and downloaded music. The iTunes store was nearly an instant hit. It not only helped the iPod dominate the market, but it also dramatically altered the economics of the entire music industry.

It is critical for board members to understand how the top management team is managing such potential external threats. Boards have a responsibility to determine how great the risk is that competitors' innovative use of IT could alter their own business's core value proposition. How does the management team evaluate the evolving IT capabilities of their competitors? What steps are being taken to ensure that the company's position and its ability to maintain margin and grow revenues are not threatened?

While the specifics of these answers will be unique to each company, management should be able to offer a structured, data-driven evaluation of these risks across product and business lines. This analysis is most helpful when supported by detailed and integrated input from business unit executives—not just from functional IT management. Scenario-based views that analyze the potential impact on revenue streams and margins across multiple business units or product lines can also be used.

If boards don't hear these elements, they should consider it a red flag. That means they need to work with their management teams to improve the corporation's ability to plan, prepare, and respond to these disruptive IT risks that can jeopardize its future.

2. Portfolio Risk: The IT project portfolio can involve hundreds, if not thousands, of independent and challenging IT projects. Generally speaking, 70% of these are dedicated to "keeping the lights on." They are business-as-usual operations—email, upgrades to existing systems, and the like. Such projects are necessary, but they won't fundamentally change the firm. The other 30% are transformational—the applications or platforms that could give your firm a big leg up on the competition. Boards need to be aware of the risk of spending too much of scarce IT dollars and resources on basic operational expenses and not enough on true transformational investments.

For a large corporation with an IT budget of approximately \$1 billion, effective portfolio management can have a huge impact on competitiveness. A firm that manages its portfolio well can reduce its "lights on" investment from the industry norms of 70% to 60% or even lower. This gain of 10 percentage points is a major competitive advantage.

Over a typical large three-year-long transformational program, that translates into \$300 million of capital available for developing new capabilities that can make or break entire product and market strategies.

It is also important to consider how the management team spreads IT dollars across the portfolio of projects to achieve an efficient risk/return ratio. According to a 2007 NACD study, over half of surveyed directors (52%) said their boards are involved in the review and approval of the information security budget¹. Boards with a high awareness of IT issues look for a structured and well-documented process for making allocation decisions, monitoring performance, and reviewing the overall portfolio. Moreover, the executive team should be able to clearly explain the trade-offs they have made. That would demonstrate they are making thoughtful and measured decisions, as well as optimizing scarce IT capital and resources.

3. Execution Risk: This type of risk involves a company not executing IT programs effectively or not delivering critical capabilities to the business on time and on budget. Because IT initiatives are often enterprise-wide, they impact many people and must be integrated with multiple technologies. They often impact client service. The failure of large programs can also cause lasting damage to brand reputation and cause companies to lose market share.

One would hope that failure is a rare occurrence. But this is not the case. As many as 70% of large IT programs don't reach their goals in the allotted time and budget, according to an Oliver Wyman estimate. Many great business strategies and plans fall apart because IT programs are poorly executed.

To manage execution risks, boards must focus on two areas: monitoring of the progress made in carrying out IT programs and insisting on their integrated management by both leaders in business lines and their counterparts in IT organizations. Management teams need to offer a thorough and consistent framework for reporting their progress in meeting IT commitments. Such a framework contains real-world IT program metrics that can act as an early warning system rather than the typical “red-amber-green” IT status reports that show everything as “green”—until the promised delivery date is close—then the reports suddenly turn “red.” If IT status reports don't show a healthy dose of “amber” throughout the program, then teams are, at best, too lenient in their judgment of their own progress. At worst, the full story is not being told for fear of repercussions.

Business and IT managers should also present an integrated view of major IT programs. If they don't, it's a warning that vast capital is being spent on IT programs without full support from business management teams.

¹ Board Leadership Series: *Information Security Oversight: Essential Board Practices*. National Association of Corporate Directors, 2007, p. 5.

The Vicious Cycle in IT

Why do IT organizations have such a difficult time supporting rapidly changing businesses? And why does the problem seem to be getting worse, not better?

The primary reason is a timing mismatch: To be successful, a business has to react quickly to changes in market structure, competition, and client needs. Often, it must make sizeable course corrections from quarter to quarter. Most IT organizations, by contrast, work on an annual cycle. They aren't equipped to shift course quickly, and, despite their best efforts, IT solutions fall further behind the business each quarter.

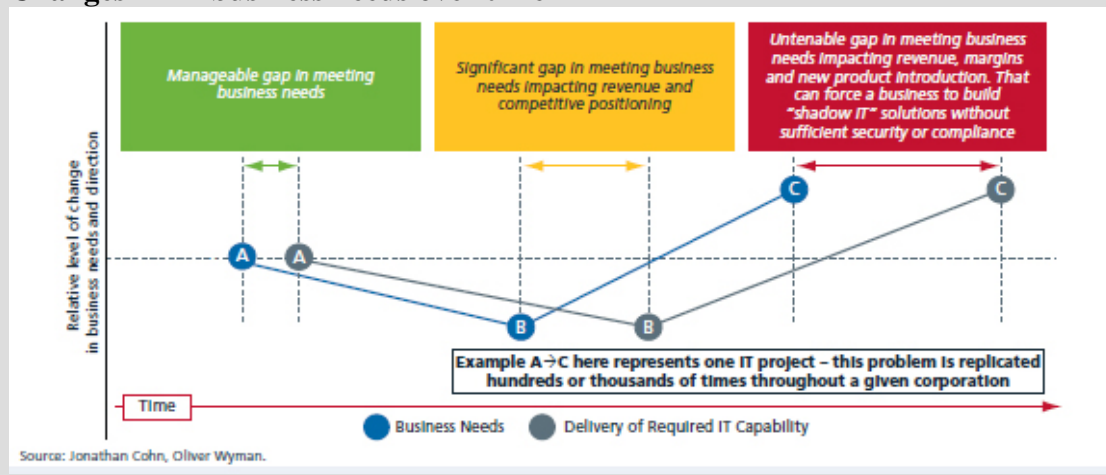
Consider the all-too-common problem of IT projects getting rolled out much later than expected. It's not that IT is lackadaisical about deadlines, or the project manager is sub-par. It happens because companies shift plans for their product, market, and trading strategies at lightning speed as the environment alters. And every time a company changes direction, the gap between what it needs as an IT solution and what IT has been working on to deliver grows disproportionately larger. (See below.)

IT teams find that they've been investing time trying to provide solutions to needs that have changed. Making minor changes to projects becomes more difficult as other altered or unfinished IT initiatives pile up behind them. Worse, some IT endeavors may never get under way, potentially forcing businesses to miss critical opportunities.

This timing problem has two other insidious affects: First, bowing to the pressure to deliver, IT groups will stop adhering to standard solutions and/or architectures, increasing the risk and support costs of a project. Second, business managers become so frustrated that they bring in "shadow IT" solutions that then must be integrated into and supported by the larger corporate IT environment.

Understanding this vicious cycle is the first step toward avoiding it. Boards should be alert to the presence of these issues within the corporations they govern. And asking tough questions of IT and business management ensures they are developing more nimble methods of designing and delivering solutions.

Changes in IT business needs over time



4. Service and Security Risk: The last category of risk refers to systems being available to keep a business—and the data within its systems—secure. Poor service levels and often painfully public security breaches of sensitive client information can alienate customers and employees as well as seriously damage a company's reputation. Yet, all too often, boards and senior executives leave these issues to their IT organizations. They need to place them squarely on their own plates.

Boards should consider how the firm invests in ongoing service and security management on a quarterly basis. Proper investments are not just in technology; they include critical employee education and process improvement that often are the weak links in overall firm security. Improving these deficiencies depend upon regular and comprehensive security assessments that include the probability of service and security breaches, prevention and remediation plans, crisis plans, and process improvement plans for areas prone to security risks.

As noted in NACD's report on information security oversight², a director's ability to detect patterns, ask incisive questions, and insist on thoughtful answers depends greatly on management's ability to provide the type of assessments described above.

It is important for boards to exercise leadership regarding security risks. They should ensure that their management teams understand that their companies' most critical information assets are constantly under threat by internal and external parties. Those who claim to have this issue solved are, at best, overly optimistic. In December, the National Security Agency announced that it now assumes all computer networks within the most secretive branch of the U.S. intelligence service have been compromised. This should alert every corporation that it is engaged in a real and unfortunate "arms race" with cyber-thieves from all corners of the world.

² Board Leadership Series: *Information Security Oversight: Essential Board Practices*. National Association of Corporate Directors, 2007, p. 8.

The Six Questions Boards Should Ask About IT Risk

Because IT touches every aspect of a company's operations, the number of questions boards could pose about technology-related decisions is nearly limitless. However, these six questions should be on every board's agenda.

- How do you determine the strategic importance of IT to the business?
- How do you evaluate the evolving IT capabilities of competitors that could threaten our industry position?
- How do you allocate dollars across the portfolio of IT investments to ensure an efficient risk return?
- What trade-offs are you making in managing the IT portfolio?
- How are you effectively executing on major IT programs?
- How do you ensure that a breadth of best practice capabilities and processes are in place to protect the firm from operational and security risks—both now and in the future?

Conclusion

Technology is changing the way businesses operate in exciting ways, and at breath-taking speed. Yet now more than ever, companies need the counsel of their boards to help them navigate a rapidly-changing environment.

Unfortunately, as our survey shows, many board members are frustrated with their ability to oversee IT risk. Whether it's due to a lack of technical expertise, insufficient information coming from management, or that old chestnut, lack of time, many boards don't offer the same sort of guidance and pushback that they do in other areas of corporate performance.

That has to change. Boards must begin demanding the information they need, and management must start presenting a picture of IT that is integrated with their view of their business. By using a common framework to think about IT risk, board members will have a shared lens through which to assess their position and a solid platform from which to take actions that benefit the corporations and shareholders they serve.