



Creating Stakeholder Value in the Information Age

The Case for Information Systems Governance

ADVISORY

AUDIT ■ TAX ■ ADVISORY

© 2004 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved.

Contents



- 1 Executive Summary
- 2 Introduction
- 4 Defining IS Governance
- 7 The Value of IS
- 9 Improving Your IS Governance
- 14 Appendix

Executive Summary



Sarbanes-Oxley, risks, controls, compliance. These are some of the most common terms being used in many board-rooms these days. They join the old favorites of value and performance.

The landscape of corporate governance has changed immensely since the emergence of recent corporate failures and resulting legislation and regulations. The sheer volume of new requirements, coupled with responsibilities placed by legislation and stakeholders, is overwhelming C-level executives, board members, and audit committees.

The simple message about information systems governance is that it needn't be complicated. After all, the Information Systems (IS)¹ department is no different than any other part of an organization and thus should be governed with the same diligence and control focus that is exercised in other areas of the organization, such as finance and human resources. Unfortunately, many discussions about IS (and its governance) are often disjointed, laced with lingo, and muddled by unclear messages, which only serves to bewilder the very people who need to understand how to govern IS. Many common business concepts, such as a common language, defined decision making and accountability structures, and reporting processes, if applied to IS would assist greatly in the governance of the IS function. When asked how they do it, executives at businesses with good corporate governance have a common answer: Run IS like a business and you'll be governing IS as it ought to be governed.

Some key concepts to bear in mind are that IS governance:

- Is an inseparable element of good corporate governance
- Is the responsibility of board members and executives (both business and IS)
- Requires a top-down approach, and senior management to live the model
- Aligns IS objectives with business objectives

Because IS governance must be an inseparable segment of good corporate governance, a business cannot have good corporate governance without good IS governance. The payoff is tangible. A 2003 study of 1,600 companies conducted by the research organization Governance Metrics International showed that businesses with strong governance structures outperform those with weak ones in terms of shareholder return.

However, if a global survey conducted by KPMG International early in 2004 provides any indication of current conditions in the marketplace relating to how businesses are assimilating IS governance measures with overall corporate governance, then much work is left to be done.

This paper focuses on the impact of recent changes on governance over the organization's IS. It stresses the importance of balancing the new requirements of controls and compliance with those of value and risk in order to assist in achieving sustainable growth. The paper concludes with some practical steps that can be followed by the organization to improve its IS governance.

In a global survey conducted by KPMG International early in 2004:

- Only 50 percent of respondents said they believed IS governance was an integrated part of their organizations' corporate governance structure.
- Only 50 percent said they believed there are risks in not aligning IS with the company's overall business goals.
- Eighty-three percent said there is room for improvement in the company's IS governance structure.
- Only 59 percent said their organization took corporate governance seriously.

¹ The terms *Information Systems (IS)* and *Information Technology (IT)* are often used interchangeably to describe the same function. For the purposes of this document the term *Information Systems (IS)* will be used.

Introduction

For many organizations, governing information technology and integrating it with the company's overall corporate governance has become a confusing and daunting duty for senior executives and board members. Discussions on the subject often are disjointed, laced with lingo and muddled by unclear messages, which only serves to bewilder the very people who need to understand how to govern IS. As a result, the

business value created when a well-governed IS function is aligned with overall business goals remains unrealized. CIOs stand to lose credibility with their colleagues on the executive committee, and the view that IS is a black hole into which funds are sucked is perpetuated.

But things don't need to be that way. CIOs, along with others in management and board members, are crucial to governing IS and integrating information technology into a company's overall business goals. Yet because so many CIOs and their colleagues struggle to clearly communicate, CIOs regularly are disconnected and isolated from senior management and board members.

The influence of many CIOs at the board level has declined and they often find themselves marginalized. Part of the fault for their marginalization often lies with CIOs themselves. They slip into

techno-speak in discussions with non-technical CEOs and board members, when simple declarative sentences about costs, progress, and projects would do. On the other hand, CEOs and board members must share in the blame for not demanding plain English from their CIOs and for not clearly articulating how they define the value they expect from their investment in IS.

CIOs frequently do not have, nor do they often seek, the kind of training in finance and business management that would serve them well in conversations with their non-technical colleagues. For their part, CEOs, and especially board members, all-too often cover their ears when the subject of anything even remotely related to IS is broached at meetings.

CEO and Board IS Governance Checklist

- Does IS have the appropriate level of representation on the executive management committee?
- Do non-executive directors understand the key IS risks facing the organization?
- Have clear and separate accountabilities for IS governance and IS management activities been assigned?
- Have IS strategies been agreed and understood by both IS and the business unit management?
- Has the business agreed on objectives and performance metrics for IS that include measurement of the value that IS generates?
- Does the same project governance operate for both IS and business projects that involve all the key stakeholders?
- Does IS operate with the same risk management processes as the rest of the business, and how formal are the processes—for example, is audit involved when major changes are being made?
- Are education programs in place to ensure the business gets the most value from IS?
- Does IS management understand the business strategy and priorities and reflect these in its decisions?

The remedies won't be easy, but a first step might be the creation of a board-level IS oversight committee, much like the audit and compensation committees already in place on many boards.² Such a decision could elevate the importance of IS governance by sending a message to the organization, its investors, and other stakeholders that the business is aligning IS governance with the company's business goals.

Top executives need to understand how value will be derived from the use and management of IS, and they need to be presented with understandable metrics that measure value. Unfortunately, many CIOs, CEOs, and board members can neither define nor measure IS value. And, when value can't be defined or measured, a business almost always will have poorly designed IS governance.

If there is a simple message about IS governance, it is that it needn't be—and shouldn't be—complicated. After all, information technology is no different than any other part of a business and thus should be governed like any other part of a business. Because IS governance must be an inseparable segment of good corporate governance, a business cannot have good corporate governance without good IS governance.

It is necessary to understand that value derived from IS for one segment of a business isn't necessarily the same as it is for another. Part of the reason for that difference is that departments seldom speak the same language, and they define value in different ways. Where one department sees value in speed, another values growth, agility, or accurate forecasting.

But in study after study about good IS governance, the common theme is that information technology should be managed as any business would manage finance, marketing, production, human resources, and other "business" functions. When asked how they do it, executives at businesses with good corporate governance say: Run IS like a business and you'll be governing IS as it ought to be governed.

If there is a simple message about IS governance, it is that it needn't be—and shouldn't be—complicated. After all, information technology is no different than any other part of a business and thus should be governed like any other part of a business.

² *CIO Insight*, February 1, 2004; "Richard Nolan: A Committee of One's Own."

Defining IS Governance



In essence, IS governance is about achieving three things:

1. Getting the most value from IS, including moving it toward its strategic goals
2. Ensuring that stakeholders and management understand the key IS risks and manage them
3. Establishing the conditions that allow IS management to operate effectively

The survey among a cross section of industries revealed that only half of the respondents believed IS governance was an integrated part of their organization's corporate governance structure. The same percentage (50 percent) said they believed there are risks in not aligning IS with the company's overall business goals. Further, more than 8 in 10 respondents (83 percent) said there is room for improvement in their company's IS governance structure.

In the networked, connected, and digitized commercial world, IS increasingly has become the backbone of a business. Consequently, the company's executive management and its board must have a clear corporate governance design that provides for good IS governance. In order for a business to produce value for its customers—whether the customers are external or internal—those who manage and operate the business must align IS objectives with business objectives. Straightforward, clear questions must be asked; frank, uncluttered answers must be given.

What IS Governance Is:

- An integral part of corporate governance
- The responsibility of board members and executives
- A mechanism to deliver value, manage performance, and mitigate risk
- A method to assign accountability for decisions and performance
- Dynamic in alignment to business goals
- Policies, procedures, management committees, performance metrics, and related management techniques working in unison toward common business goals

At Vroom & Dreesmann Department Stores in The Netherlands, CIO and CFO Albert Balvers says, "IS is treated as a normal part of ongoing business. We look at different performance indicators, among which are the financial indicators, and we have an IS steering committee, consisting of business managers and IS managers. We have formal and informal agreements about the services delivered and mutual expectations are clear and transparent. The business as well as IS can be held accountable for not following up on agreements. The emotion is taken out of the discussion and has been replaced by facts and figures."³

Over the past decade, boards and senior management around the world have spent an increasingly larger share of their capital expenditure funds on IS. Some estimates are that IS expenditures represent at least 40 percent of capital expenditures in business today.⁴ But academics and industry observers suggest that despite its ubiquity in business, IS and how to govern it remain broadly misunderstood and under-appreciated.

For example, in its publication, "*Board Briefing on IT Governance*," the IT Governance Institute suggests that board members must turn their attention to IS governance.

"While boards usually look at business strategy and strategic risk, few boards have focused on IT, despite the fact that it involves large investments and huge risks. Why is that? Among the reasons:

- IT requires more technical insight than do other disciplines to understand how it enables the enterprise and creates risks and opportunities.
- IT has traditionally been treated as an entity separate to the business.
- IT is complex, even more so in the extended enterprise operating in a networked economy."

³ KPMG interview, 2004.

⁴ *Financial Times*, July 13, 2004, "Warnings Cast Doubt on Strength of Capital Spending."

“IS governance just happens in many enterprises,” according to Marianne Broadbent, in *“Designing Effective IT Governance,”* a 2003 Gartner Inc. publication.⁵ In those enterprises, “IS governance is not actively designed to achieve business objectives and desirable behaviors.”

When a business integrates good IS governance into its corporate governance practices, it promotes the creation, understanding, and acceptance of an enterprise-wide vision of the value of IS. At its core, good IS governance provides a mechanism to execute strategy and a way to measure performance against goals. In order for IS governance to be effective it must be communicated well. “Decisions, obligations, and relationships can be defined, but if they are not communicated effectively, or supported through living the model, such definitions can be disruptive, confusing, and counter to the purpose for which they were first conceived,” says Ludo Vandervelden, vice president of the Information System Group at Toyota Marketing Europe. “Time, budget, and quality are all urgent issues addressed by the IS governance model; if you fail the model, you are most likely failing the business as well.”⁶

Triggered by fraudulent corporate failures and shoddy governance, law-making bodies around the world in the past two years have created, or are toughening, legislation aimed at rooting out corruption to protect shareholders and stakeholders. At the same time, shareholders and stakeholders are demanding that business leverage IS in order to deliver value. Still, many people inside and outside a business have no idea what delivering value through better IS governance means, let alone how to do it. And even fewer can measure it.

When IS governance works, decision-makers in an organization understand it and they work within defined roles toward a common goal. When it fails, roles are misunderstood, people are confused, and goals and opportunities are missed. “Having a governance model in place gives you an immediate return,” Vandervelden says. “However, like all things with great potential for benefit, governance improperly or inadequately done can be worse than none at all.”

In their book, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, co-authors Peter Weill and Jeanne W. Ross report that they studied 256 businesses and found that only 38 percent of senior executives at those businesses could accurately describe their IS governance. The authors then split that group of businesses into top performers and bottom performers, based on a basket of financial performance metrics. Firms in the top third of performance had more than 50 percent of senior executives, sometimes as high as 80 percent, who could accurately describe their IS governance. In the poorer firms, fewer than 20 percent of the senior executives could describe their IS governance.⁷

There appears to be two schools of thought on what IS governance is about. On one hand, IS governance often is said to be the process of how and where decisions about IS are made. On the other, some organizations view IS governance as a focus on risk management and controls.

What Good IS Governance Does:

- Aligns IS objectives with business objectives
- Provides a way to measure performance against goals
- Mitigates risks
- Delivers value
- Helps ensure that business solutions are delivered on time and within budget
- Assists in delivering professional IS service to the enterprise

What Good IS Governance Is Not:

- A compliance issue
- Only the responsibility of the CIO
- Only about technology
- Only an IS strategy
- An isolated discipline or activity
- A static framework
- Just an IS steering committee function

⁵ Gartner Inc., 2003, “Designing Effective IT Governance.”

⁶ KPMG interview, 2004.

⁷ Harvard Business School Press, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*.

Because both views have merit, it is important that businesses striving for improved IS governance incorporate both in their IS governance efforts. The key to successful IS governance is getting the right balance between value, risk, and cost-effective IS performance.

A number of academic and professional bodies have sought to provide more structure for IS governance in recent years. As the level of corporate failures, or perhaps the visibility of these, has grown, so the business world has sought to standardize and develop more sophisticated techniques for addressing these issues. Frameworks such as Control Objectives for Information and Related Technologies⁸ (COBIT) and the IT Infrastructure Library⁹ (ITIL) have been developed from either accounting or

government backgrounds to provide some structure and the formality of leading practices to these issues.

According to the KPMG International survey, techniques such as COBIT and ITIL are used effectively by less than 20 percent of organizations. About one-third of our respondents consider themselves to be effective in the use of external benchmarks. With the considerable focus on IS governance, it is surprising that the apparent adoption has not been more widespread.



⁸ COBIT is a registered trademark of the IT Governance Institute. Copyright 2000.

⁹ ITIL is a registered trademark of the IT Service Management Forum. Copyright 1996.

The Value of IS



“According to the META Group, 70 percent of IT organizations are still perceived as cost centers rather than value centers, and 52 percent of CEOs question the value their IT departments deliver.”

“Completing the IT Value Equation,”
May 18, 2004,
Enterprise Applications Pipeline,
CMP Media LLC

Because there is no simple way to define IS value, and since value means different things to different people, it is best to let the IS function’s customer describe their own vision of value. With that, IS will have a foundation on which to build a relationship that can lead to the delivery of value. In other words, know the customer by learning what they need from IS, and then learn how to tell the stories of successes across all departments. “Marketing is absolutely critical to being internally successful,” Stephen Norman, COO of Merrill Lynch’s technology group, said in the May 1, 2004, magazine interview. “We live in a world where by and large our customers don’t understand what we do. So we need to market internally to have a shot at building partnerships and avoiding surprises.”¹⁰ Traditionally, IS functions are poor at marketing themselves.

Effective communications and marketing IS inside an organization may help avoid the trap into which CIOs and other IS executives so often fall: Telling a customer how IS value will be delivered, rather than asking the customer to define the value they are seeking and then working to deliver it.

Effective value creation from the delivery of IS is subjective. One of your customers may only be interested in how quickly data gets delivered or analyzed. Another may see value when IS helps to contain costs or comply with corporate governance legislation. Yet another may be satisfied if their system is agile. Still others may want to make certain that forecasting will be precise.

Despite years of pronouncements at many corporations that IS spending would only be permitted when there is an alignment with the delivery of business value, things clearly are still out of kilter. According to the META Group, 70 percent of IS organizations are still perceived as cost centers rather than value centers, and 52 percent of CEOs question the value their IT departments deliver.¹¹

In many major corporations, according to *Harvard Business Review* authors Charlie S. Feld and Donna B. Stoddard, “IS is an expensive mess. Orders are lost. Customers call help desks that aren’t helpful. Tracking systems don’t track. Indeed, the average business fritters away 20 percent of its corporate IS budget on purchases that fail to achieve their objectives, according to Gartner Research. This adds up to approximately \$500 billion wasted worldwide.”¹²

At the same time, there are top-tier companies that reliably deliver a stream of projects that provide value to the business and assist them in achieving the leading market positions. With ingrained good governance these well-run companies quickly identify when projects start to drift; problems are identified and reported on; and joint decisions are made on whether to continue to invest to make them succeed, or to cut the losses and cancel them.

¹⁰ *CIO Magazine*, May 1, 2004, “The Secret Weapon: Internal Marketing.”

¹¹ *Enterprise Application Pipeline*, CMP Media LLC, May 18, 2004, “Completing the IT Value Equation.”

¹² *Harvard Business Review*, March 15, 2004, “Fixing the Corporation—IT Disconnect.”

Effective communications and marketing IS inside an organization may help avoid the trap into which CIOs and other IS executives so often fall: Telling a customer how IS value will be delivered, rather than asking the customer to define the value they are seeking and then working to deliver it.

The pay-off for good governance is tangible. A 2003 study of 1,600 companies conducted by research organization Governance Metrics International showed that businesses that have strong governance policies outperform those with weak ones in terms of shareholder return. Because of that payoff, businesses increasingly are using IS auditors, internal and external, to check that their IS governance is in place and operating efficiently.

Noted IS observer and author Nicholas Carr reinforces the very important point that, whether or not an organization believes that IS adds value to the firm, IS executives need to start figuring out how to measure and demonstrate that the IS function adds value or they will see their IS budgets dwindle. The easy days of IS funding, if there was such a thing, are gone. Enterprise resource planning (ERP) systems, Y2K, and e-business have impacted the credibility of IS, and it is becoming increasingly difficult to credibly justify that the next IS development will change the world. Instead, CIOs need to consistently deliver return on investment (ROI) on IS investments so that the business will be asking for the next opportunity to save it money or improve its operation. This point was driven home recently in a *BusinessWeek* magazine article, which noted that spending on IS must occur along “with organizational changes to achieve real productivity gains.” In the same article, Hewlett-Packard CEO Carleton S.

Fiorina noted, “CIOs will spend money on information technology only to raise ROI.”¹³

While it is easier said than done to consistently deliver ROI on IS investments, that is the challenge that faces the person in the CIO’s hot seat. And, it is the responsibility of the CEO to support his or her CIO to meet that challenge.

Measuring the Successful Delivery of IS Value:

- Use of a scorecard for internal customer service
- Regular and vigorous review of IS projects by the executive committee
- Updated and validated industry benchmarks
- Performance against service-level agreements with customers
- Portfolio management tools that identify overlap and underutilization

¹³ *BusinessWeek*, February 9, 2004, “Harmony and Belly Dancing at Davos.”

Improving Your IS Governance



Improving IS governance within the IS department falls on the shoulders of the CIO, who must champion and sustain governance efforts within the IS management team.

Getting good at, or better at, IS governance takes time, persistence, and a methodical plan that starts with the recognition and acceptance that good governance is critical for building and sustaining a great organization. To get to a place where good IS governance is part of the fabric of a business, an organization must:

- Obtain the necessary sponsorship. This means that it is not only the CIO who supports a good IS governance environment, but also members of the board and all of the executive management team.
- Understand the organization's current IS governance environment by asking such questions as:
 - What are our IS governance mechanisms?
 - What is the business context in which IS operates?
 - How are decisions made on IS spending?
 - Does the business have an effective risk management program?
 - How satisfied are your customers? And, how do you know their level of satisfaction?
 - Do you have rigorous and consistent processes and responsibilities for running IS, developing and improving applications, ensuring business continuity, purchasing, managing staff, budgeting, creating business value, and aligning your IS strategy with your business strategy?
 - Where are the gaps?
- Create a design for moving to where you want to be with IS governance. The plan should include:
 - Agreement on what business value is expected and how it should be measured
 - A list of short-term, medium-term, and long-term projects to improve IS governance over time
 - A way to increase the maturity of your application-development process
 - Ways to ensure buy-in from all levels of the organization
 - A schedule to meet with business units and agree on how and where decisions are made for IS investments
 - A review of your process for customer feedback
 - A schedule to update and communicate your IS policies and procedures

Broadly, the ways to improve IS governance can be categorized into two groups—those improvements that occur between the business segments and the IS department, and those that occur within the IS department itself. The improvements between IS and the business segments are the responsibility of the board and C-level executives—including the CIO. Improving IS governance within the IS department falls on the shoulders of the CIO, who must champion and sustain governance efforts within the IS management team. The success of IS governance measures depends entirely on the governance mechanisms that bond IS to the business strategy.

Communication

A powerful tool to improve IS governance—clear and consistent communication—is simple and obvious. Yet, at many organizations the board and C-level executives do not fully understand IS and its value to the organization. They are typically apprehensive about discussing IS with the CIO out of a fear of appearing ignorant. Well-governed

businesses do not allow this hurdle to be placed in the path of their business goals because CIOs have a clear understanding of the business goals and how IS can help reach them. Furthermore, the executive management team at these businesses does not view CIOs as service-delivery specialists. Instead, the CIO is a member of executive management who has learned how each member of the management team expects IS to deliver value, and then works to help ensure that those expectations are met.

Clear and consistent communications help companies “run IS like a business.” When the CIO is grounded in the language that non-technical executives use, there is a good chance that he or she could explain the progress of a project in a way that the CIO’s colleagues in executive

management can immediately understand. When a board or executive management asks a CIO to explain the progress of a project they probably don’t want to hear about the complexities of implementing middleware to enable the mainframe to relay data to the Web front-end. If a CIO and his or her executive management colleagues have worked hard on communications, the CIO might answer the question with a description of a project’s return on investment, its necessary business-process changes, or the project’s milestone analysis.

Tools to Improve IS Governance



Source: KPMG LLP (U.S.), 2004.

“IT is the next disaster waiting to happen. ... [IS oversight committees] are responsible for ensuring a continuous dialogue takes place between top management and the people in the IT department.”

Richard L. Nolan,
Professor Emeritus,
Harvard Business School

IS Oversight Committee

Communication regarding IS decisions and execution does not begin and end with the executive committee. A board of directors that does not have members who understand the scope and impact of their company’s IS is at risk. Much like the current focus on having financial experts on audit committees in the wake of high profile corporate failures, there is now discussion that more companies should take that idea a step further and create an IS oversight committee. Because the investment in IS has been significant for many years, shareholders and stakeholders are asking questions on how IS is overseen and managed.

Harvard Business School Professor Emeritus Richard L. Nolan, who currently sits on several corporate boards and is an advocate of IS oversight committees, says he believes “IT is the next disaster waiting to happen.”¹⁴ IS oversight committees, he says, “are responsible for ensuring a continuous dialogue takes place between top management and the people in the IT department.”¹⁵

¹⁴ *CIO Insight*; February 1, 2004; “Richard Nolan: A Committee of One’s Own.”

¹⁵ *Ibid.*

Following decades of significant spending on IS, and because a large portion of capital investment of an average company is now going into information technology, senior management is obliged to pay more attention to governing IS than it has in the past, he says. “That’s not the only reason—and maybe not even the most significant reason—to get boards involved,” Nolan says. “The role of IT is expanding both deep within organizations and across organizations. The notion of a firm’s boundaries has changed: Companies have become permeable, and decisions affect entire networks of companies. Meanwhile, every organization today is absolutely dependent upon IT ... IT activity has evolved so rapidly that it now has a future-shock kind of impact. Senior management is not really up to speed on their degree of dependence on IT, or on IT’s impact and strategic potential. It’s an accident waiting to happen. Someone needs to intervene, and the board is the best mechanism for rendering this much needed top-down leadership.”¹⁶

Agreement on Objectives

Good governance is frequently characterized by formal agreements between providers and users of information technology. These so-called service-level agreements (SLAs) can be useful when they use business measures to describe the service that is to be provided. Good service level agreements use language that both the users and the providers agree upon, and they provide a basis for understanding and improving the service that is offered.

These agreements are powerful tools for IS to understand the real requirements of the business users and for IS to report their performance back to the business users in a form that is understandable and useful to them.

Many organizations may claim to have service level agreements in place between the IS function and the business, but in many cases, these are technical in nature and actually enforce the language divide between IS and the business rather than bridging it. Useful agreements are phrased in business terms and aimed toward the real business user’s requirements of the systems. For example, the business user would rather know that the HR system was 95 percent available rather than that the UNIX server was 95 percent available or that the network was 96 percent available.

Although writing the agreements is time-consuming at the front end, well-constructed agreements can provide value by having an IS function that is aligned with true business requirements. Once an organization understands the role of these SLAs, many cannot understand how they functioned effectively without this critical link between IS and the business.

Organizations that perceive users of IS as customers and seek their feedback will improve the possibilities for developing good governance. Measuring customer satisfaction may be an annoyance when done too frequently, but an effective customer feedback system can help pinpoint areas that need attention.

Although writing the agreements is time-consuming at the front end, well-constructed agreements can provide value by having an IS function that is aligned with true business requirements.

¹⁶ Ibid.

Breakdown Stress Points

When there is a breakdown in IS governance, and thus in overall corporate governance, the failure frequently can be traced to familiar stress points. These include:

- The thinking throughout the organization that IS governance is a one-time project. There is no quick fix in the pursuit of good IS governance. It is a process, not a project.
- Where IS is treated differently in other elements of the organization in achieving the overall business goals.
- When IS is looked upon solely as a cost-cutting mechanism instead of an enabler of business value and a way to improve the operation.
- When a particular business function dominates the IS department's resources and efforts.

At a time when systems often are distributed across vast geographic boundaries, well-defined and accepted policies can help avoid the risk of individuals seeking their own solutions to fit their IS needs without consideration of the overall corporate strategies.

IS Strategy

One of the key governance mechanisms that the IS organization can put in place is a clear IS strategy. Although it is frequently the CIO's responsibility to develop this strategy, it cannot be developed in isolation. Clear links ought to exist between the IS strategy and the overall business strategy. Consequently, members of the entire executive committee need to have detailed discussions with the CIO about their views on the IS strategy.

The executive committee as a group should decide how the business should be positioned with respect to the use of IS, and whether the organization wants to be a technology leader or a follower in its industry. Justifications needed for major technology investments can thus be associated with this positioning. The IS strategy provides a road map for developing IS infrastructure and systems that will support the business in achieving its goals. The strategy typically includes the hardware and software to be used and how IS strategies will be deployed. The strategy also must have sufficient flexibility to respond to unexpected changes in business direction, but also be sufficiently specific to serve as a basis for communication and performance measurement.

Policies, Procedures, and Standards

Well-governed businesses almost invariably have well-defined IS policies, procedures, and standards. These powerful management and governance techniques are the tools that provide a business with a road map toward better governance.

Policies are the practical arm of the IS strategy. They allow management to interpret the strategy into practical elements by guiding members of the IS function in terms of the procurement, development, and acceptable usage of IS as laid out in the IS strategy. Furthermore, policies allow management to document its requirements in terms of items such as data security and change management. IS policies may help ensure that staff members are aware of their respective duties and responsibilities, and thus underscore a vital aspect of governance—agreement on where and how decisions are made about IS in the business.

At a time when systems often are distributed across vast geographic boundaries, well-defined and accepted policies can help avoid the risk of individuals seeking their own solutions to fit their IS needs without consideration of the overall corporate strategies.

Procedures and standards take policies to the next level of depth by helping to establish practical means of ensuring that the IS function runs in a repeatable and understandable fashion. Procedures and standards assist management in gaining comfort that the specific process or function is being performed in a consistent manner. They also allow management to gain perspective of the controls in place within a process, while at the same time assisting in facilitating job sharing and continuity of functions.

Accountability

During the development of the policies and procedures for the IS function, it is critical that the accountability for IS decisions be defined. Accountability is one of the cornerstones of good governance, and responsibility for elements of IS governance must be assigned.

Although overall accountability for IS should be assigned to someone at a suitable level of responsibility in the organization, it is necessary to assign a range of accountabilities within the IS function to support the overall governance. Accountability should be defined within the company's IS policies and procedures, which should be linked to the principles of communication and transparency. Much of the current corporate governance legislation and standards around the world require transparency of governance, making the clear delineation of accountability imperative.

Performance Management

To assist management with an understanding of how well the IS processes are running, a good system of measuring performance should be in place. When established at realistic levels and communicated appropriately, performance standards and metrics give employees a clear definition of expectations and a goal to work toward.

Good performance management systems often will include a broad understanding among staff and executive management about the business requirements of IS. Often the understanding will come from well-defined and accepted service level agreements. Specific metrics are critical to success because they produce data that link performance to the business service being provided.

Risk Management

A rigorous risk management process helps enable a business to identify and understand risks associated with IS that may have a negative impact on the business. When identifying risks, the business impact needs to be understood. Once a risk is identified management can decide what to do with the risk along four dimensions:

- **Avoid the risk.** Make a decision that might enable the organization to avoid a risk altogether.
- **Accept the risk.** Be aware of the risk but not do anything about it other than monitor it.
- **Mitigate the risk.** Reduce the likelihood or consequences of the risk.
- **Transfer the risk.** Involve a third party to take on some of the impact of the risk, e.g., insurance.

Project Management

Due to the constant quest to improve technology, a number of large projects are frequently underway within IS at any point in time. Good project management assists the organization in implementing projects that are in scope, within time and cost constraints, of sufficient quality, and able to be integrated to the applicable business processes and related systems. Many organizations rely on a project risk management function that runs alongside the traditional project management function to identify and analyze risks to the project and to recommend risk mitigation techniques to management. Others apply techniques such as portfolio management to balance priorities and spending rather than managing one project at a time.

Ultimately, an effective IS governance program will allow a business to demonstrate and continuously improve its management of information assets in support of its business goals.

Key Points to Remember

IS Governance:

- Is an inseparable element of good corporate governance
- Is the responsibility of board members and executives (both business and IS)
- Requires a top-down approach, and senior management to live the model
- Aligns IS objectives with business objectives
- Promotes the creation, understanding, and acceptance of an enterprise-wide vision of IS's value
- Provides a mechanism to execute strategy and a way to measure performance against goals
- Is a mechanism to deliver business value, manage performance, and mitigate risk
- Serves as a mechanism to direct people, processes, and technology to a common goal
- Gives a business the ability to make rapid moves in today's globally competitive marketplace
- Is a method to assign accountability for decisions and performance
- Should be tailor-made for your business: one size does not fit all
- Closes expectation gaps between IS and its stakeholders

Appendix



Members of KPMG's Information Risk Management practice recently interviewed several executives about IS governance and how their businesses create and manage IS governance. Following are the edited versions of some of those interviews:

Ludo Vandervelden, Vice President, Information Systems Group, Vehicle Logistics Group, Business Process Improvement Office, Toyota Motor Marketing Europe.

KPMG: How do you define IS governance?

Ludo Vandervelden (LV): IS governance is a set of rules and understandings that you document between parties in an organization. It is where you establish interrelationships and responsibilities for executing tasks according to a defined strategy. Governance is multi-dimensional, rather like an onion. At the core, you have governance within your immediate boundaries defining relationships. And, within this, [you have a] definition of tasks, roles, and responsibilities. You also ensure management and control mechanisms, and define clear objectives and participation.

KPMG: What relationship do you see between IS governance and corporate governance?

LV: There is a very strong relationship between corporate governance and that of IS. Corporate governance defines the core or middle of the onion, with additional layers dependent upon the complexity of your organization. At each of these layers, governance clearly defines the understandings, interactions, and agreements in how you conduct your business.

Corporate governance is thus the starting point for IS governance, as it establishes the basic roots of the company. It defines the complexity of the company, and establishes both our internal organizations and our relationships with our national marketing companies. Corporate governance provides the essential architecture of the business, and from this broad picture, we define our IS strategy in sync with those processes.

In our structure in Europe, it was clear that the first aspect of IS governance we had to put in place was between IS and the business units. This derives from our corporate governance, where we established that there are business units and internal organizations like IS.

KPMG: How effective do you consider IS governance to be in your organization?

LV: We had initial difficulties with IS governance in two areas. The first was that we had start-up issues regarding the cooperation of all parties. The business perceived IS as being expensive. External vendors, however, did not fully understand our company's requirements, and all costs were not included in outside vendor proposals. This led the business to believe we were unrealistic and expensive. Our value was better clarified when the business realized that money expended to outside vendors was not resulting in the IS solutions it needed. Its experience helped discipline the organization.

We have installed an extension to our IS governance model called Office of Excellence, a joint project-driven structure for business IS. We started the program in the most difficult areas—often where outside vendors were used—and it is bringing results.

The second problem has to do with attendance at governance meetings, primarily due to the unavailability of people. We're making progress here by incorporating discussions and decisions regarding charge-out rates and budget into the meetings. This has enhanced their importance and made them a priority. The meetings are becoming more effective over time, but we still have a way to go.

KPMG: *What, in your opinion, makes effective IS governance?*

LV: Involve all parties in its evolution, be responsive to changes in strategy and business, require all parties to live the model, synchronize with corporate governance and strategy, and—perhaps one of the most important—ensure consistent and continuous communication. Governance requires living according to the established rules. Depending upon the complexity of your organization, the implementation of IS governance requires a staged approach and clear understanding at all levels of the organization.

KPMG: *What business benefits have been gained from implementing your IS governance structure?*

LV: The short answer is that it has provided for reductions in costs, with the end result being our ability to reduce our charge-out rates to the businesses. This has come about through the transparency that IS governance has given operations, along with enhanced credibility.

IS governance has given us an instrument for influencing important cost factors and in setting our priorities. It simply saves time. One of the biggest elements—and risks—in IS is in estimating costs of projects when available resources are not known. IS governance helps you to define all the elements in preparing valid quotes, going a long way toward better credibility with the businesses. It has enhanced our operations, given us tools for cost control, reduced adverse budget impacts, and helped make all parties more accountable. It has enhanced the maturity of our organization.

KPMG: *Do you consider that IS governance is an effective tool that most organizations do or should have?*

LV: IS governance is important to us, as it regulates relationships and avoids conflicts and misunderstandings. The IS governance document is a contract between people. It provides a road map defining our roles and responsibilities. It's a basic document—like a constitution—regulating the rights and obligations of all parties involved.

All organizations require clear definitions of tasks and responsibilities. As this is inherent in most governance models, it follows that all organizations could benefit from incorporating IS governance where it would be appropriate. That said, if your model doesn't define mutual and individual responsibilities, its effectiveness is greatly diminished. Most of the companies in Europe who are facing, as we are, a history of decentralized local representation, and who now need to go for economies of scale, can only do so if they have a clear understanding up front of who is responsible for what.

KPMG: Are there cultural differences in the implementation or its effectiveness?

LV: Yes, to the extent that culture influences the adoption of the tenets of IS governance, and the understandings relating to its successful implementation. For example, Toyota's National Marketing and Sales Companies, like many businesses and institutions in Europe, have a history of independent action that has challenged the adoption of a more centralized approach. We have to be sensitive to this history while gaining the benefits of economy of scale brought about by centralization and consolidation of effort.

KPMG: What processes and procedures have you put in place that you consider to constitute your IS governance framework?

LV: More than four years ago, we defined an IS governance paper that outlined the tasks of the business and rules of IS. Through discussions with the business units, and based on the core governance draft, we gained an understanding of what IS had to do within the organization. These rights and responsibilities, once negotiated and approved by all the business unit leaders, comprised the final document submitted to the executive committee. The approved governance now forms the basis of all discussions and relations between IS and the business units. It also forms the basis for budgeting and planning, capital investment, scoping, business case preparation, and the mechanism for communications.

KPMG: Are traditional concepts such as board representation in place?

LV: Part of our IS governance requires periodic meetings with executives to review progress, adjust our priorities, and make essential decisions regarding investment, projects, budgets, and allocation of resources. Part of this is also reviewing our success in meeting the obligations we have accepted in the governance model, and ensuring that we are still in alignment with corporate strategic objectives.

KPMG: Are these truly effective in the current climate?

LV: IS governance provides us with a plan for a professional, methodically structured organization that can respond to the responsibilities we have accepted. This is important. As I said previously, it enhances the maturity of our organization. That said, a great deal of effort and energy is put into effectively using the tools given us through governance. IS governance is a starting point for developing an IS strategy, a road map; it must be traveled to be effective. Anyone who puts IS governance in place and doesn't structure his organization accordingly to comply with what he promises is burned out very fast. You have to live it and you have to do it.

KPMG: Does corporate management perceive IS governance as a cost or a value-added process?

LV: IS governance does not cost you lots of money. If you look at the rules and structures you put in place, they don't cost a lot in comparison with what you can lose. Having a governance model in place gives you an immediate return. However, like all things with great potential for benefit, governance improperly or inadequately done can be worse than none at all.

KPMG: *If any of the business is outsourced, what additional governance procedures are required?*

LV: Standards are very important. Indeed, if you outsource business, then you need additional governance procedures. But we are not entirely there yet. We do incorporate service level objectives and service level agreements in our IS governance model, but some homework remains to be done. In some areas we are well advanced, in others, not so.

KPMG: *What challenges to organizations do you see from your experiences in implementing your governance structure?*

LV: Challenges from incorporating IS governance reside more in the risks of not doing it well. Decisions, obligations, and relationships can be defined, but if not communicated effectively, or supported through living the model, such definitions can be disruptive, confusing, and counter to the purpose for which they were first conceived. Time, budget, and quality are all urgent issues addressed by the governance model; if you fail the model, you are most likely failing the business as well.

KPMG: *How can these be overcome?*

LV: There is only one way to overcome challenges to IS governance: provide proper and consistent communications and make the necessary investment in management time and energy. Good communications are essential to successful cooperation and buy-in from all participants. I would emphasize that the benefits of IS governance are very important and justify this commitment. To those who would be concerned about any risk in adopting IS governance, I would say: the underlying, basic reason for IS governance is that there are more risks without it.

Albert Balvers, CIO/CFO of Vroom & Dreesmann Department Stores, discusses IS governance and how it impacts his organization.

KPMG: *How do you define IS governance?*

Albert Balvers (AB): IS governance is the set of rules and agreements, formal or informal, written down or not—intended to govern the decision-making—the who, what, when, why—regarding the information supply within the organization.

KPMG: *What relationship do you see between IS governance and corporate governance?*

AB: They are two inseparable items. The same rules and framework apply for IS governance as for corporate governance. Corporate governance is the starting point to answer the question: How does corporate governance translate into governance for the various parts of the organization? IS is just one of those parts. Since governance is also about culture, ethics, and adapting to internal and external circumstances and influences, it cannot be seen as separate from the information supply within the organization. Therefore, corporate governance and IS governance are integrated.

KPMG: *How effective is IS governance in your organization, and, in your opinion, what makes effective IS governance?*

AB: Our IS governance is becoming more and more effective. From a situation in our organization where business was business and IS was IS, there is now a situation where the business side takes responsibility for defining its requirements regarding strategy, planning, and operational use of IS.

Now that IS is treated as a normal part of ongoing business we look at different performance indicators (among which are the financial indicators), and we have an IS steering committee consisting of business managers and IS managers. We have agreements (formal and informal) about the services delivered, and mutual expectations are clear and transparent. The business as well as IS can be held accountable for not following up on agreements. The emotion (IS image) is taken out of the discussion and has been replaced by facts and figures. The business owns the IS budget and determines how this budget is spent in supporting the business.

KPMG: *What business benefits have been gained from implementing your IS governance structure?*

AB: Some of the benefits are transparency and clarity about roles and responsibilities. IS is therefore a business-supporting component instead of a “techno” driven development. The direct business benefits are: processes operate more fluently, the availability of our products in the stores is higher than it was ever before, and actions trigger a predictable reaction instead of waiting for surprises to happen.

The business is able to manage and steer on output, rather than on emotion and educated guesses. Governance and IS governance resulted in a more efficient, but simple, dashboard for performance indicators, and therefore there is a clear basis for accountability. (RACI matrix is used.)

KPMG: *What processes and procedures have your organization put in place that you consider to constitute your IS governance framework? Are traditional concepts such as board representation in place? Are these truly effective in the current climate? How have these drawn on the academic theories such as COBIT and ITIL?*

AB: It is most important that the business take responsibility for integrating IS in its operations. On various levels in the organization, from the board down to operations, there are meetings with various frequencies. These meetings extend to external IS suppliers as well. IS governance requires, however, a top-down approach and the involvement, commitment, and power of the board is needed to implement and maintain governance. IS governance requires a good balance between entrepreneurship—freedom and risk-taking—on the one side and achieving operational excellence by standardized, fine-tuned (formal) procedures on the other side.

KPMG: *Does corporate management perceive IS governance as a cost or a value-added process?*

AB: If corporate governance and IS governance are implemented well they will deliver their value. Although in the beginning it might feel that the more formal structures that are required for good governance are limiting maneuverability, this is not the case. If implemented well, the structures provide a solid base and effective ways to operate day-to-day business.

KPMG: *What challenges have your organization confronted in implementing the governance structure? And, how were they overcome?*

AB: Three major challenges are:

1. The need for a vulnerable attitude

When implementing governance with its procedures, (a company's) responsibilities and performance become clearer, but one has to have a vulnerable attitude. If one is afraid to be held accountable, or to admit that in the past governance was a problem, then the implementation of corporate governance procedures is likely to fail.

2. Shooting from trenches

When results are becoming clear, and one is working toward agreements that have not been made before, there is a great chance of people shooting at each other when something goes wrong or is not completely in line with the agreements that have been made. Instead of shooting each other from the trenches, people have to be working together to find solutions for the problems and challenges that arise.

3. Leadership from the top

Implementation of IS governance needs a strong hand from a strong leader. Although many business changes can be implemented with a bottom-up approach, the implementation of governance is a top-down change. Leadership has to show the importance of the governance structure and live by it. Since governance is part of corporate culture, it should be practiced as preached from the top down. Leadership has to set an example, day after day.

Robin Dargue, CIO and Business Process Director of Diageo, a premium drinks business.

KPMG: *How do you define IS governance?*

Robin Dargue (RD): We see it covering five dimensions: oversight of change projects; management of the IS functions; link to the executives and the board; funding of strategic change and securing the IS assets, such as IS security; and disaster recovery planning and ensuring a stable IS environment.

KPMG: *What relationship do you see between IS governance and corporate governance?*

RD: I see two key linkages: Firstly, ensuring the security of IS assets. By assets I include the people, data, and infrastructure—everything that IS is accountable for. Secondly, it is the link to the business executive to ensure a two-way alignment of the strategies.

KPMG: How effective do you consider IS governance to be in Diageo? What are the key success factors?

RD: We are getting better at it, I think for two key reasons. Firstly, we have the right forums in place with the right attendees. We have an Audit and Risk Committee composed of the most senior business executives. This committee covers all business risks, including IS. We then have an IS quarterly business review, which I chair and which is attended by the most senior business executives. This lasts half a day, and we cover our performance promise for IS, IS people and talent issues, and make strategic IS decisions. Finally, we have an Executive Working Group that oversees business change and major programs, whether they involve IS or not.

The second reason is business empathy. I see my role as key to nurturing this. I think the CIO has to have the ability to listen, understand the business issues, and recognize the different points of view. With the latter, it is important to distinguish between different views on “what” to do and “how” to do it. In addition, IS has to be transparent and honest about problems and issues—this builds credibility and support. I try to ensure that we educate the business so that it can see what IS is doing and how IS contributes to our strategy.

KPMG: What business benefits have been obtained from these IS governance mechanisms?

RD: The value to IS has been that we do not have any “knee jerk reactions” or “management by budget.” We can now have a wider debate on funding. For example, last year there was a gap in our budget and we were able to reverse a decision to delay global projects at the expense of local programs. The value to the business is that it has a great channel for value-added ideas and opportunities.

KPMG: Do you consider that IS governance is an effective tool that most organizations should have? Are there cultural differences in its implementation?

RD: Yes it is very important. I think the implementation depends on the organization. For example: Who is accountable for IS? A geography or a central IS function? I see two extremes of IS governance—at one end, a focus on the IS delivery aspects, and, I think, most people I see are at this end. The other extreme is a focus on IS strategy. The trick is to get the balance right, and we are trying to lean more toward the IS strategy end.

KPMG: Did you put in place any additional IS governance procedures when you outsourced?

RD: Yes. We have a separate Strategic Account Review every six months with both IBM and Accenture. We look at performance against the service levels and then we ask each company to give us value-added ideas to discuss. I see this as a sort of “safety valve.” The top-level relationship is between these organizations and myself. If they want to speak to my executives and I agree, then I will arrange it and go along.

KPMG International

KPMG is the global network of professional services firms of KPMG International. Our member firms provide audit, tax, and advisory services through industry-focused, talented professionals who deliver value for the benefit of their clients and communities. With nearly 100,000 people worldwide, KPMG member firms provide audit, tax, and advisory services from 715 cities in 148 countries.

Major KPMG Contributors

Egidio A. Zarrella, Sydney, Australia
Mark T. Lindig, New York, NY, United States
Bryan Cruickshank, Edinburgh, United Kingdom
Armin Weyell, Frankfurt, Germany
William Carr, Houston, TX, United States
Mark R. Puzey, Perth, Australia
Gaston Vankan, Amstelveen, Netherlands
Coert Scholte, Antwerp, Belgium
Clive Webb, London, United Kingdom
Andrew Dunkinson, Montvale, NJ, United States
Patrick Ryan, Montvale, NJ, United States

Written by Timothy R. Dougherty, Montvale, NJ, United States

Graphic Design by Carole Law, Atlanta, GA, United States

Visit KPMG on the World Wide Web at www.kpmg.com.

The views and opinions are of those interviewed and do not necessarily represent the views and opinions of KPMG member firms.

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG International is a Swiss cooperative that serves as a coordinating entity for a network of independent member firms. KPMG International provides no audit or other client services. Such services are provided solely by member firms in their respective geographic areas. KPMG International and its member firms are legally distinct and separate entities. They are not and nothing contained herein shall be construed to place these entities in the relationship of parents, subsidiaries, agents, partners, or joint venturers. No member firm has any authority (actual, apparent, implied, or otherwise) to obligate or bind KPMG International or any member firm in any manner whatsoever, or vice versa.

© 2004 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved. Printed in the United Kingdom. 26635atl

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

kpmg.com