Why IT governance is a top management issue
Lainhart, John W, IV
The Journal of Corporate Accounting & Finance; Jul/Aug 2000; 11, 5; ProQuest
pg. 33

Why IT Governance Is a Top Management Issue

John W. Lainhart IV

Information Technology (IT) used to be just an enabler of corporate strategy. No more. Now it's an integral part of it. But how do you implement a sound IT governance plan? One professional organization has some answers.

As a result of today's fast-paced, global technology advancements, many experts estimate that business conducted over the Worldwide Web will reach US $1 trillion before 2005. On the other hand, Computer Economics, an independent research firm, recently found that the economic impact of virus attacks on information systems around the world reached US $12.1 billion in 1999.

There is no question about it—today's economy is an information economy. Because the future growth and success of business rely on taming information technology for secure, profitable use, it's often a case of two steps forward, one step back.

GOOD GOVERNANCE EQUALS GOOD BUSINESS

Companies striving for success in this environment must integrate information technology (IT) with business strategies to attain their business objectives, get the most value out of their information, and capitalize on the technologies available to them.

Effective enterprise governance focuses individual and group expertise in specific areas where it can be most effective, monitors and measures performance, and provides assurance to critical issues. IT was once considered solely an enabler of an enterprise's strategy. Now it is regarded as an integral part of that strategy. CEOs, CFOs, and CIOs alike agree that strategic alignment between IT and enterprise objectives is a critical success factor.

IT governance helps ensure achievement of this critical success factor by efficiently and effectively deploying secure, reliable information and applied technology.

According to the Governors of the Central Banks of the G10, effective governance provides proper incentives for management to pursue objectives that are in the interests of the enterprise, its stakeholders , and the public. It also ensures that management has the appropriate tools and abilities to achieve the enterprise's objectives. Governance arrangements provide accountability to owners and to the wider community, so those served by the business can influence its overall objectives and performance. Above all, governance systems must be transparent, so all affected parties have access to information about decisions impacting the enterprise.

Simply put, good governance—enterprise and IT—is good business.

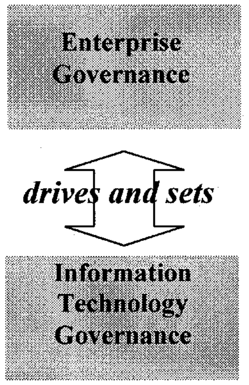
GOVERNANCE RELATIONSHIPS

Enterprise governance, the system by which companies are directed and controlled, drives and sets information and technology governance. At the same time, IT should provide critical input to, and form an important component of, strategic plans devised for enterprise governance. IT may in fact influence strategic opportunities outlined by the enterprise. (See Exhibit 1.)

Enterprise activities require information from IT activities to meet business objectives.

Exhibit 1

IT Governance Is a Two-Way Street



Successful organizations ensure interdependence between their strategic planning and their IT activities. IT must be aligned with and enable enterprises to take full advantage of information. (See Exhibit 2.) By so doing, they maximize its benefits, capitalize on opportunities, and gain a competitive advantage.

HOW ENTERPRISE GOVERNANCE WORKS

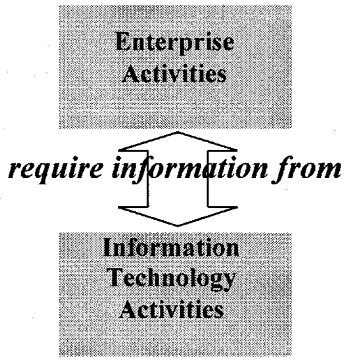
Enterprises are governed by generally accepted good (or best) practices, the assurance of which is guaranteed by certain controls. From these practices flows the organization's direction, which dictates activities. The enterprise's activities use its resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls...beginning the cycle again. (See Exhibit 3.)

IT GOVERNANCE MIRRORS ENTERPRISE GOVERNANCE

IT governance functions in much the same way as enterprise governance, although in a more focused arena. Like the enterprise itself, IT also is governed by good (or best) practices. These practices are designed to ensure that the enterprise's IT resources are used responsibly, its risks are managed appropriately, and its information and related technology support its business objectives. Best practices also direct IT activities, which can be characterized as planning and organizing, acquiring and implementing, delivering and supporting, and monitoring—all undertaken for two purposes: managing risks (to gain security, reliability, and compliance) and realizing benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again. (See Exhbit 4.)

Exhibit 2

Good Governance Means Independence



But IT governance is not an arcane set of theoretical principles. Active and inclusive, it encompasses:

- Capital resources (information systems, technology, and communication);
- Strategies and regulations (business, legal, and other issues); and
- Human resources (all concerned stakeholders, including directors, senior management, process owners, IT suppliers, users, and auditors).

WHAT'S THE BIG DEAL?

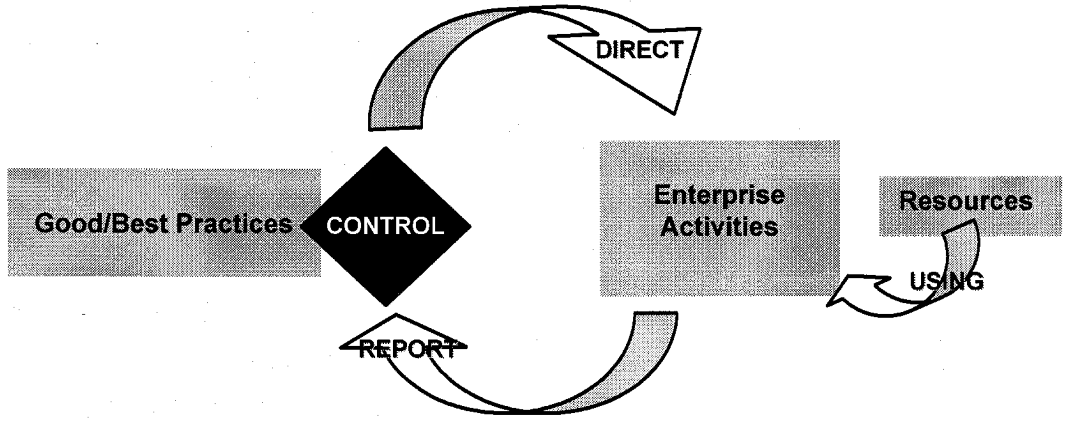
Why should anyone care about IT governance? And why now?

IT governance is a big deal because it enables an enterprise to more effectively address major business issues such as enterprise resource planning (ERP) and electronic commerce. It helps the business ensure the security, reliability, and integrity of its strategic information. It protects the enterprise's investment in information technologies, including systems and networks. And, it ensures the appropriate management of the enterprise's information assets, which often are directly responsible for the success and survival of the enterprise itself.

If these reasons weren't enough for embracing the importance of IT governance, there are specific situa-

Exhibit 3

How Enterprise Governance Works



tions—opportunities and threats—in the business environment right now that should prove powerful motivators for implementing good governance principles. Effective IT governance enables an enterprise to take advantage of current business opportunities and avoid impending business threats.

OPPORTUNITIES AND THREATS

Opportunities exist in the demand for better stewardship for businesses. Enterprise stakeholders are no longer content to sit back and let the business run itself. They want an active role in its management, they want to be a player in its decisions. Most of all, they want assurance that those who run the enterprise on a day-to-day basis are taking all possible steps to protect the business and make the best use of its assets. Enterprises demonstrating that assurance—and an IT governance plan is one way of doing so—can reap the rewards of stakeholder support.

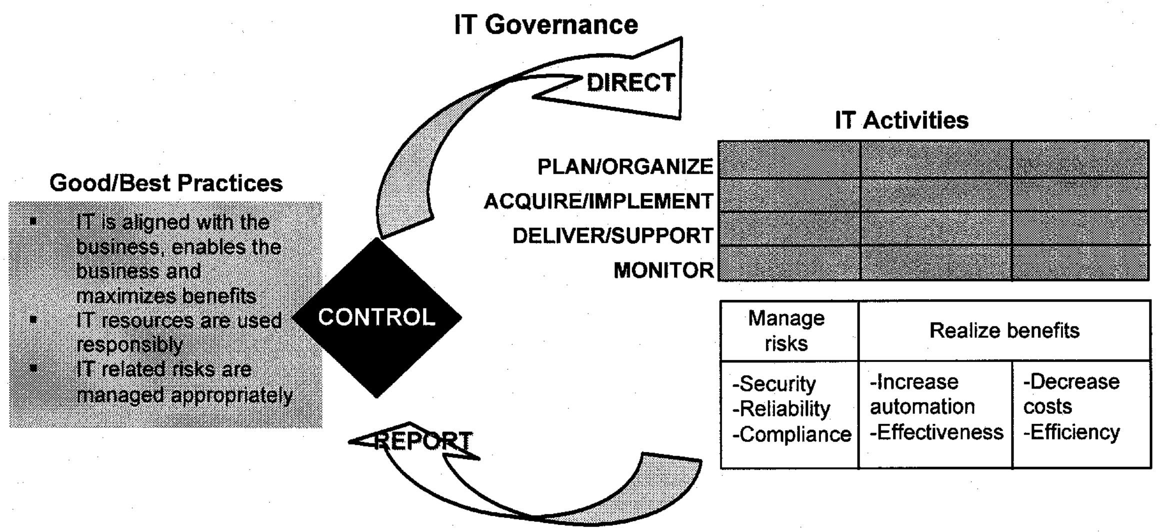
Electronic commerce is another huge business opportunity that seemingly everyone is exploring today. Electronic commerce requires an enterprise to be able to show effective control of IT and information to trading partners and customers. Without the trust of partners and customers, companies do not have a chance of succeeding in the rapidly burgeoning electronic commerce arena. IT governance enables businesses to inspire that trust, through clearly demonstrated control over the IT function.

Business threats are just as numerous as business opportunities. Perhaps the most rampant are increased security threats and vulnerabilities, through information warfare and cyberthreats. Rarely a day goes by that evidence of hacking or illicit data manipulation isn't trumpeted in the press.

A Russian hacker using the name Maxus, for example, took 300,000 credit card numbers from an Internet music Web site and held them for ransom. When the music company refused to pay the US $100,000 ransom, Maxus posted 25,000 of the credit card numbers to a Web site.

Only a week after this incident, a news story on APBnews.com revealed that a group of British hackers attempt-

Exhibit 4



- IT is aligned with the business, enables the business and maximizes benefits
- IT resources are used responsibly
- IT related risks are managed appropriately

Manage risks	Realize benefits	
-Security -Reliability -Compliance	-Increase automation -Effectiveness	-Decrease costs -Efficiency

ed a US $10 million extortion of VISA International. Confident that its security systems had protected customer credit card information, VISA contacted Scotland Yard and the FBI. A VISA spokesman emphasized that the hackers were not able to access any transactional processing systems.

In addition to security concerns, there is a need for improved controls by which enterprises protect and standardize their IT activities. Many control systems currently in place are a patchwork of stopgap measures, developed in an uncoordinated and unstructured way to deal with specific short-term situations. Most businesses need an integrated, interdependent, comprehensive set of controls by which their IT functions can operate.

Along with controls, there is a need for internationally accepted best practice standards guidance. The economy is now global and there is a demand for consistency and transportability across differing systems, processes, and regulatory environments.

In each of these cases, IT governance, with its sound plan of continually monitored and measured activity, can help companies avoid potentially disastrous threats.

ENTER *COBIT*

With opportunities knocking and threats looming, it is more crucial than ever for an enterprise to implement a sound IT governance plan. The Information Systems Audit and Control Foundation has published an IT governance tool that helps nontechnical managers understand and manage risks associated with information and related IT. Called *Control Objectives for Information and related Technology (COBIT) 2nd Edition*, this comprehensive framework of control objectives is based on 36 international source documents, ensuring a global view and a "best practice" point of view.

COBIT consists of an Executive Summary, a Framework, and 34 high-level Control Objectives, supported by 302 detailed Control Objectives. (These three sections are available for download from the International Systems Audit and Control Association [ISACA] Web site, as an open standard:

www.isaca.org.) Supporting the high-level Control Objectives are Audit Guidelines and an Implementation Tool Set, featuring case studies and various management and IT diagnostic tools.

COBIT has a strong business focus. It is designed for business process owners as well as users and auditors. *COBIT* helps managers communicate and bridge the gap with respect to control requirements, technical issues, and business risks. It facilitates the development of clear policy and good practices for IT control throughout an organization, worldwide.

> *DaimlerChrysler has incorporated the COBIT Framework and the Control Objectives into its internal controls standards database for use in audit planning throughout the world by IT auditors based in Germany and the United States.*

COBIT AT WORK

Patricia Earl-Cole, principal auditor for Blue Cross Blue Shield of Michigan (BCBSM), has implemented *COBIT* within her organization and found it an effective tool for just that sort of management/IT communication.

BCBSM supplies health care benefits across the United States and has approximately 8,200 employees. Its systems process nearly 75 million claims annually, representing US $7 billion in benefits provided.

According to Earl-Cole, implementing *COBIT 2nd Edition* has increased management's awareness and support of controls. Because of the improved communication among diverse groups, management has made a conscious effort to focus on development and application of controls, and demonstrates a more profound understanding of how control recommendations affect business functions.

"*COBIT* is an immensely useful tool to help bridge the IT communication gap among executive management, IT, and audit," said Earl-Cole. "Nearly every organization could benefit from *COBIT* to help make sound control decisions based on IT processes and the business functions they support."

And, in fact, many other organizations have implemented *COBIT*. DaimlerChrysler has incorporated the *COBIT* Framework and the Control Objectives into its internal controls standards database for use in audit planning throughout the world by IT auditors based in Germany and the United States. The Central Bank of Argentina has adopted *COBIT* as a guideline for IT minimum controls and *COBIT* is to be implemented in information technology examinations. The U.S. Federal Financial Institutions Examination Council (FFIEC) has adopted a revised Uniform Rating System for Information Technology (URSIT), which uses *COBIT* as a guideline for IT controls and is to be implemented in information technology examinations of all banks and data processing service providers. The U.S. General Accounting Office's Federal Information Systems Control Audit Manual includes *COBIT* references in every section. And, the U.S. Critical Infrastructure Assessment Office has defined a Vulnerability Assessment Framework for Federal Government agencies that references *COBIT* as the basis for its IT control framework.

OBSTACLES AND PITFALLS

Because it is so comprehensive, *COBIT 2nd Edition* cannot be taken off the shelf and applied wholesale to any environment. IS auditors, managers, and business process owners must all make the effort to tailor the document's advice as appropriate for their environment. Not all control objectives - high-level or detailed- will be appropriate within each enterprise. The type of industry the business is in may affect which sections are applicable. Quite often, the size of the IT staff itself can come into play. For example, *COBIT* may recommend that certain functions be divided among several individuals, for cross-checking and control purposes, while in a small IT staff, such division of responsibilities is impossible.

COBIT is designed to be generic enough to be applicable to any type of hardware or software environment. Therefore, some enterprises may choose to customize the information, making it specific to exactly their own platform.

IT GOVERNANCE SELF-ASSESSMENT

COBIT 2nd Edition provides an additional tool to help companies get started evaluating their own IT governance systems. The IT Governance Self-Assessment checklist (see Exhibit 5) leads management to determine the following for each of the *COBIT* processes:

- How important the process is for their business objectives;

Exhibit 5

COBIT IT Governance Self-Assessment

Risk		**Importance** - how important for the organization, on a scale from 1 (not at all) to 5 (very) **Performance** - how well it is done, from 1 (don't know or badly) to 5 (very well) **Audited** - Yes, No or ? **Formality** - is there a contract, an SLA or a clearly documented procedure? (Yes, No or ?) **Accountable** - Name or "don't know"		Who Does It?						Who is accountable?
Importance	**Performance**	**COBIT's Domains and Processes**		**IT**	**Other**	**Outside**	**Don't Know**	**Audited**	**Formality**	
		Planning and Organization								
		PO1	Define a Strategic IT Plan							
		PO2	Define the Information Architecture							
		PO3	Determine the Technological Direction							
		PO4	Define the IT Organization and Relationships							
		PO5	Manage the IT Investment							
		PO6	Communicate Management Aims and Direction							
		PO7	Manage Human Resources							
		PO8	Ensure Compliance with External Requirements							
		PO9	Assess Risks							
		PO10	Manage Projects							
		PO11	Manage Quality							
		Acquisition and Implementation								
		AI1	Identify Solutions							
		AI2	Acquire and Maintain Application Software							
		AI3	Acquire and Maintain Technology Architecture							
		AI4	Develop and Maintain IT Procedures							
		AI5	Install and Accredit Systems							
		AI6	Manage Changes							
		Delivery and Support								
		DS1	Define Service Levels							
		DS2	Manage Third-Party Services							
		DS3	Manage Performance and Capacity							
		DS4	Ensure Continuous Service							
		DS5	Ensure Systems Security							
		DS6	Identify and Attribute Costs							
		DS7	Educate and Train Users							
		DS8	Assist and Advise IT Customers							
		DS9	Manage the Configuration							
		DS10	Manage Problems and Incidents							
		DS11	Manage Data							
		DS12	Manage Facilities							
		DS13	Manage Operations							
		Monitoring								
		M1	Monitor the Processes							
		M2	Assess Internal Control Adequacy							
		M3	Obtain Independent Assurance							
		M4	Provide for Independent Audit							

© 1998 Information Systems Audit and Control Foundation
Reprinted with permission.

- Whether the process is well performed (the combination of importance and performance provide a strong indicator of risk);
- Who performs the process and who is accountable for the process (and whether accountability is unequivocal and accepted);
- Whether the process and its control are formalized; that is, is there a thorough contract for an outsourced activity or a clear set of documented procedures for an internal process; and
- Whether the process is audited.

> *COBIT 2nd Edition is currently being updated to make it an even more effective IT governance tool.*

Completion of this checklist heightens management's awareness of the combination of risk indicators, degree of formality and clarity of responsibility and accountability. High-risk indicators combined with "Don't know" answers relay a strong message of concern.

When areas of high risk are identified, management can concentrate on these, using *COBIT*'s high-level and detailed control objectives and working with their IS auditors to determine cost-effective means for mitigating these risks. As a result, the enterprise's IT governance is enhanced and true value-added benefits accrue to the entire enterprise.

COBIT UPDATES

COBIT 2nd Edition is currently being updated to make it an even more effective IT governance tool. Management Guidelines, in the form of critical success factors, key goal indicators, key performance indicators, and maturity models, are being added. These Management Guidelines are intended to provide management tools to assess and measure their organization's IT environment against *COBIT*'s 34 IT processes.

Critical Success Factors (CSFs) define the most important issues/actions for management to address for achieving control over and within its IT processes. They are management-oriented implementation guidelines that identify the most important things to do, strategically, technically, organizationally, or process/procedurally.

Key Goal Indicators (KGIs) are measures that tell management an IT process is achieving its business requirements. These measures are those management would like to see on their "dashboard" and comprise measures for the process itself as well as measures of performance (*Key Performance Indicators* [KPIs]) of the IT processes. KPIs are expressed in terms of capabilities, practices, and skills that enable the process to achieve its goals; and KGIs are usually expressed in terms of the information criteria:

- Availability of information the business needs;
- Absence of integrity and confidentiality risks;
- Cost efficiency of processes and operations; and
- Confirmation of reliability, effectiveness, and compliance.

Maturity Models measure how well developed management processes are. They provide the means to perform self-assessments, allowing an organization to grade itself from very poor (0) to excellent (5)—similar to the approach used by the Software Engineering Institute in its Capability Maturity Model, defined for the maturity of the software development capability.

The Maturity Models provide a theoretical measurement scale for each of *COBIT*'s 34 IT processes and allow management to map the:

- Requirements of the most stringent emerging international standards/regulations;
- Current status of the organization;
- Current status of best-in-class organizations in the industry; and
- Organization's strategy for targeted improvement.

The interaction among these Management Guidelines can be summarized as follows: CSFs suggest what you need to do based on the choices made in the Maturity Models, while monitoring through KPIs whether you will likely reach the IT process goal set by the KGI.

Over the next few years, enterprises will have to demonstrably attain increasing levels of security and control. Every enterprise must understand its own performance and must measure its progress. Using the Maturity Models for IT control, organizations can benchmark themselves and measure their progress against peers and strategy in an effort to achieve a competitive level of IT security and control.

Management Guidelines such as these will provide management with the answer to its perpetual question: "What is the right level of control for my IT such that it supports my business objectives?"

INSTITUTIONALIZING IT GOVERNANCE

IT governance is a fairly recent term. It has only been in the past decade or so that the increasing dependence of business on IT and the risks that dependence entails have become clear. This growing awareness has led organizations to recognize that if they are to make the most of their investment, and protect that investment at the same time, they need a formal process to govern it.

Acknowledging the increasing importance of effective IT governance, a new entity, the IT Governance Institute, has been established. The Institute exists to clarify and provide guidance on current and future issues pertaining to IT governance, control, and assurance. Consisting of individuals who possess both business and IT expertise, the IT Governance Institute will undertake original research, convene symposia, conduct trend analysis, and pursue other activities designed to benefit professionals and enterprises impacted by the effective control of information and related technologies.

One of its first undertakings was the creation of a Web site dedicated to IT governance. Located at www.ITgovernance.org, the site contains an overview of IT governance and a wealth of resource material and links to other pertinent sites. An IT governance framework and a publication explaining IT governance to Audit Committees are in development.

WHAT'S NEXT?

There is no reason to believe that the need and demand for effective IT governance will fade anytime in the near future. The reasons for implementing an IT governance plan show no signs of disappearing:

- Increasing dependence on information and the systems that deliver the information;
- Increasing vulnerabilities and a wide spectrum of threats;
- Scale and cost of current and future investments in information and information systems; and
- Potential for technologies to dramatically change organizations and business practices, create new opportunities, and reduce costs.

As long as these factors remain in play, there will be a need for effective, interdependent systems of enterprise and IT governance. A few years ago, *The McKinsey Quarterly* issued a report indicating that two-thirds of investors would pay more (up to 16 percent) for the stock of an enterprise that was perceived to be well-governed. Their reasons: They believe that well-governed companies will perform better over time, thereby increasing share value, and that businesses with effective governance plans manage risk better and rebound from setbacks more quickly. Capital chasing governance: now *that's* tangible proof that good governance—enterprise and IT—is indeed good business.

John W. Lainhart IV is a partner with the Washington consulting practice of PricewaterhouseCoopers in Washington, D.C. In this capacity, he focuses on providing management consulting services to federal, state, and local governments and the services industries.