Chapter

19

IT Governance: Toward a Unified Framework Linked to and Driven by Corporate Governance

David Pultorak

Introduction

At the time of this writing, the industry has yet to sort out the precise nature of IT governance. IT governance remains an evolving concept within an evolving concept: that of corporate governance. The old adage, "What you see depends on where you sit," describes precisely where we are in the discourse around the nature of IT governance. Existing perspectives on the nature of IT governance include the following:

1. IT managers and specialized IT staff tend to see IT governance as a mechanism for aligning business and IT at the level of the program office, projects, and significant IT investments and architectural decisions.
2. IT Auditors tend to see IT governance as a control mechanism to ensure compliance with relevant authorities and to manage risk to the business.
3. IT service management professionals tend to see IT governance as ensuring IT services are aligned to current and future business needs, meet quality objectives as perceived by the customers, and are managed for efficiency and effectiveness.
4. Corporate board members and top managers sometimes do not know what to make of IT governance (just as they are sometimes at a loss for what to make of IT in general) and have in some cases abdicated responsibility for IT governance.

Except in the last instance, there is nothing inherently wrong with any of these perspectives. What is wrong and dangerous is an over-focus on one perspective or the persistence in the organization of multiple, unaligned perspectives. For example, many organizations coping with Sarbanes-Oxley start to see corporate governance solely as control around financial reporting and pay little regard to other aspects of governance. The operational reality in many of today's organizations is that IT governance is conducted as an unaligned set of activities based on a mix of competing micro-theories, the unintended consequence of which is the creation of the very inefficiencies and risk exposures that governance mechanisms are intended to address.

This chapter looks at IT governance from a perspective and scope that is different from what is common today. It takes the position that IT governance, properly construed, is a *discipline* within corporate governance, and as such, the board's perspective should be primary and the board should be the ultimate driver of IT governance. As a discipline within corporate governance, IT governance activity should be directed in the dimensions important to corporate governance: Conformance, Performance, and Relating Responsibly (CPR), where

- Conformance is ensuring that the corporation meets relevant regulatory requirements.

- Performance is ensuring that the corporation achieves its performance objectives.
- Relating responsibly is paying appropriate attention to relevant stakeholders.

We start by briefly recounting the evolution of the concept of corporate governance. We then outline a three-part CPR framework for board-directed governance and provide guidance on how to implement the CPR framework for IT governance.

Corporate Governance: An Evolving Concept

In the wake of the previously unthinkable business debacles that marred the early days of this century, everyone seems to acknowledge the need for corporate governance. But what *is* corporate governance, precisely? Specifically, *who performs it, to what end, and by what means?* At times there seem to be as many answers to these questions on the nature of corporate governance as there are people talking about it. As shown in Table 19.1 and outlined in the paragraphs that follow, while the end game of corporate governance has not changed, who performs it and by what means has evolved considerably from traditional concepts.

Corporate Governance: Unchanging End, Changing Means

Historically, the end game of corporate governance has been sustained financial results *by means of a focus on financial management*, so much so that in the recent past, corporate governance was virtually synonymous with the measuring, monitoring, and reporting of the financial condition of the enterprise. While focus on sustained financial results is an appropriate and timeless end, the landscape upon which business is conducted has changed such that the *means* to achieving that aim must change in a number of important ways. The paragraphs that follow outline how the business landscape has changed and how the means of governance must change to fit that landscape.

Table 19.1 Toward a New Concept of Corporate Governance: The CPR Framework

Corporate Governance	Performer	End	Means
The traditional concept	The board, top management, financial auditors	Sustainable financial results	Avoidance of realization of risks to financial results through control
The CPR framework	The board, all management, a variety of auditors, all staff, external entities	Sustainable financial results	Managing and leading for results in three dimensions: CPR for the four assets any business must govern: infrastructure, clients and external stakeholders, internal people and process, value creation

Today's organizations are complex, distributed, networked entities in a complex, distributed, networked marketplace. In the past, it might have been possible for a single person or small group of people to "get the whole system in mind" and exercise governance. This is less and less feasible and is impossible in some cases. The impact is that *who performs corporate governance must change*. In the traditional view, corporate governance was the responsibility of the board and its immediate delegates (top management and financial auditors), and the focus was financial. In today's complex organizations, where the corporation's "value constellation" is made up of a constantly changing set of entities (some outside of the corporation's direct control), governance activity must be extended both down into and outside of the organization to include an expanded role for internal staff and external entities. In addition, as IT and security have emerged as significant risk areas to the business in addition to financial practices, IT and security auditors must be added to the mix.

The networked nature of today's businesses and marketplace means aspects beyond financial ones can have an immediate and lasting impact on the organization. The result is that *the scope of key performance indicators (KPIs) that must be managed to achieve sustained financial results must be expanded beyond the financials*. About a decade ago, Kaplan and Norton (1996) highlighted the fact that focusing on financial performance alone was not enough to ensure sustainable results. Kaplan and Norton dramatically extended the factors to be considered in corporate governance, recommending a balanced scorecard of governance dimensions: financial performance, business process, customer fulfillment, and learning and growth (Figure 19.1).

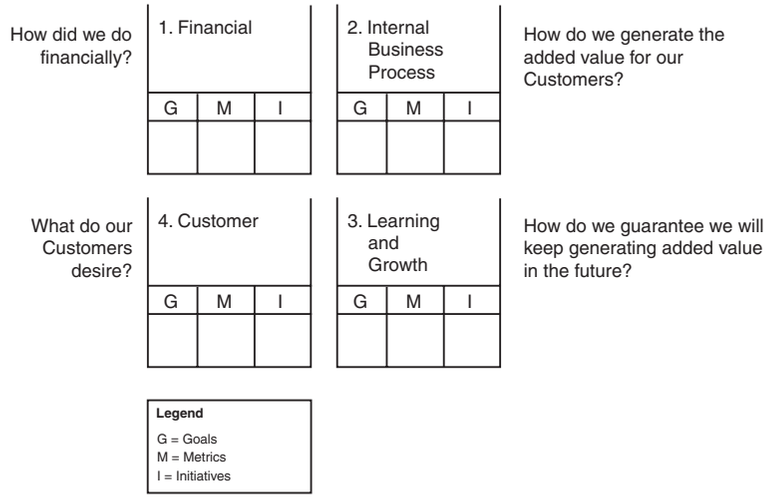

Figure 19.1 The Balanced Scorecard.

Weill and Ross (2004) highlight the object of governance as six key assets to be managed:

- Human
- Financial
- Physical
- IP
- Information and IT
- Relationship

Both the Balanced Scorecard and Weill and Ross's work are certainly contributions to the industry and useful tools to be included in any governance framework. These frameworks are working to answer the question, What are the principal assets of a firm that any business must mind in order to thrive? Pultorak (2001) attempts to update the answer to this question in the form of the Technical and Operational Architecture (TOA) dashboard, which is shown in Figure 19.2. The TOA dashboard is a technical and organizational architecture dashboard because it encompasses both the technical (infrastructure) and the organizational (clients and external stakeholders, internal people and process, value creation) architecture that all firms must have to succeed.

The TOA dashboard is intended to capture the four assets—infrastructure, clients, people and process, and value creation—that any business must manage, whether it is a bakery, a mid-market manufacturing firm, or a Fortune 500 financial services company. All businesses must have a solid infrastructure as a foundation for doing business, with high enough levels of availability given the cost required for further levels of

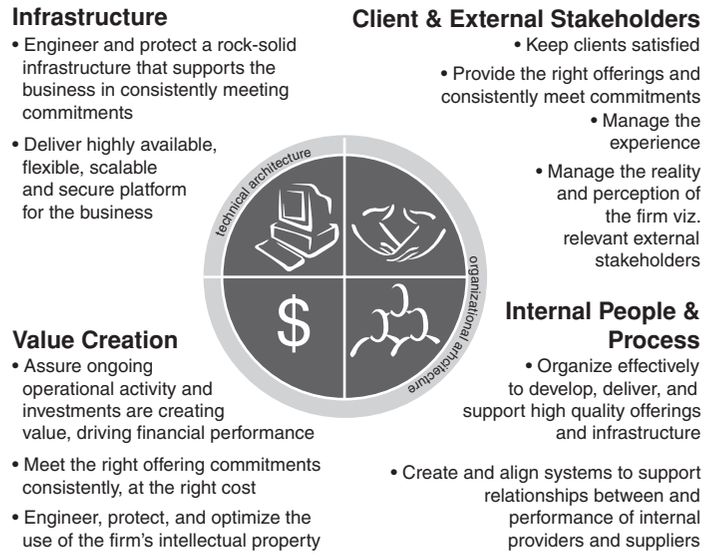

Figure 19.2 TOA: Technical and organizational architecture. The four assets any business must govern.

Source: Adapted from Pultorak, D., "Yes We Can Do It—And This Is What It Will Cost." *Presentation to the itSMF Annual Conference,* 2001, Brighton, UK.

availability. They must serve their customers in ways that make customers want to come back. They must ensure relationships with external stakeholders are maintained in a manner that enables rather than disables the business, because the organization's reputation is often its most valuable asset, the most easily lost and the most difficult to regain. They must take care of the people who serve the customer, including suppliers, and ensure that business processes are optimized. Lastly, they must ensure the value creation capability of the firm is maintained and enhanced so that the firm has the basis for driving toward business value and financial performance. The TOA dashboard in combination with the CPR framework, outlined later in the chapter, are intended to form the bones of a sound governance framework that can be used across the corporation.

In the current business landscape of highly networked enterprises in a highly networked marketplace, normal operating conditions include a relative frequency and variability of demands (opportunities and threats) that are high and increasing. In this climate, *the scope of mechanisms for achieving sustained financial results must be extended beyond merely controlling for business risk to driving toward business opportunity*. While some see risk management as including understanding and managing both negative and positive risks (positive risks being opportunities), many do not. Controlling risk is an appropriate focus, and the need for such focus is clearly increasing, but today's complex organizations may not be able to achieve sustainable results if driven solely by the avoidance of risk. Achieving sustainable results requires more than just "avoiding pain" (e.g., controlling, directing, and managing to avoid breakdowns, risks, and negative consequences); it requires "moving toward gain" (e.g., supporting and enabling positive performance, and appropriate risk-taking.) As such, a governance framework must provide a mechanism for both seeking gain (maximizing value) and avoiding pain (managing risk). Control is but one of many means to the end of sustainable results.

The business landscape of highly networked firms in a highly networked market means the number of stakeholders relevant to a firm's sustained success might be an order of magnitude greater than in a landscape that is not networked. As a result, *the scope of stakeholders relevant to sustained financial results must be expanded, and along with it, the scope of effort required to manage both the reality and perception of the corporation's functioning*. Many corporations have

stumbled as they worked toward achieving sustainable financial results for two reasons: first, they overlooked important, relevant stakeholders, and second, the way they conducted themselves "turned off" rather than "turned on" relevant stakeholders. Proper governance requires attention to both *what* you do and *how* you do it in the eyes of relevant stakeholders.

Any useful operational definition of corporate governance must address these issues. The TOA scorecard forms part of such an operational definition, identifying the four assets any business must manage in order to thrive. What is missing is the specification of the dimensions along which these assets must be managed. The CPR framework, first introduced in Pultorak (2003) and presented below, is just such a framework. The CPR framework, used in combination with the TOA dashboard, is intended as a governance framework applicable across the enterprise.

The CPR Framework for Corporate Governance

The CPR framework defines corporate governance as follows:

> Corporate governance is the systematic pattern of behavior of the board, management, and staff of a corporation that is directed toward the corporation achieving sustainable financial results. The behavior that is corporate governance must be directed toward the four primary assets of the business:
>
> 1. Infrastructure
> 2. Clients and external stakeholders
> 3. Internal people and process
> 4. Value creation
>
> by managing the current and creating the future state of the corporation by expending effort in three dimensions:
>
> 1. Conformance—to legal and regulatory requirements
> 2. Performance—financial and otherwise
> 3. Relating Responsibly—maintaining rapport with relevant stakeholders

> To ensure success, the behavior that constitutes corporate governance must be ordered within a framework established by the board that aligns and informs day-to-day decision making, objective setting, achievement monitoring, and communication.

There are a number of important distinctions made in this operational definition of corporate governance:

1. The aim of corporate governance is clear and singular: sustainable financial results. However, sustainable financial results cannot be achieved solely by directing the management of the current state of the organization; it also requires directing the organization toward its future state. The ancient Greek philosopher Heraclitus considered "becoming" as preceding "being," To him, if "becoming" should cease, then all things, including "being," would cease. Therefore, it goes with corporate governance: a governance framework that focuses on regulating the "being"—the current, steady state of an organization is not sustainable. What is required is a governance framework that propels it toward what it is to be, a governance framework that focuses on "becoming." Danny Maco (2003) echoes this sentiment by stating that ". . . what a company is now is less important than what a company plans to be."
2. Governance is primarily *behavior* that constitutes a relationship between the corporation and its relevant stakeholders. Stewardship is perhaps the best word that captures the nature of such behavior. While artifacts like systems, policies, and controls may enable (and in some cases disable) governance, they do not constitute governance itself. Governance is constituted by behavior, and it is that behavior which constitutes the relationship among relevant stakeholders, including owners/shareholders, the board, and top management. This view stands in sharp contrast to other positions on what constitutes governance, including those that see governance primarily as decision making (as behavior includes action as well as decision) or those that equate governance with its mechanisms and artifacts.
3. Effort expended on governance should be driven efficiently from the right source. The right source is the corporate board, hence the requirement in the CPR definition of corporate governance that "corporate governance must be ordered within a framework established

by the board that aligns and informs day-to-day decision making, objective setting, achievement monitoring, and communication."

The corporate governance framework set out by the board must constitute a compelling vision and a simple set of policies and procedures that serves four purposes:

- Clarifies the direction of the corporation
- Motivates people to take action in the right direction
- Prioritizes, informs, guides, and aligns the many decisions, actions, and communications made each day
- Provides a basis for monitoring progress

4. The object of governance is the four primary assets of the business: infrastructure, clients and external stakeholders, internal people and process, and value creation. Without effort along the right dimensions toward managing these assets, no business can survive or thrive.
5. Governance requires effort in the three dimensions of CPR mentioned earlier. *Conformance* means ensuring that the corporation meets relevant legislative requirements. *Performance* means ensuring that the corporation achieves its performance objectives. *Relating responsibly* means paying appropriate attention to relevant stakeholders. Effort within each dimension is necessary, but each alone is not sufficient for sustainable results. Sustainable results require more than just driving toward financial performance and more than controlling, directing, and managing to avoid breakdowns, risks, and negative consequences. Sustainable results require the supporting and enabling of positive performance, appropriate risk taking, and "moving toward gain." As such, a governance framework must provide a mechanism for both seeking gain (maximizing value) and avoiding pain (managing risk). Just managing risk is not enough. While it is certainly necessary to prevent and mitigate situations and conditions that are, or could potentially, affect performance negatively, considerable effort and focus must be directed toward creating and driving situations and conditions that would positively affect performance. How one gets there also matters a great deal, which means that building and managing the relating-responsibly aspect

with relevant stakeholders is also essential. The sections that follow describe the three dimensions more thoroughly.

The CPR framework for governance is depicted in Figure 19.3. The CPR framework includes the vital task of managing risk through controlled compliance to relevant regulatory authorities (Conformance). However, effort in two additional dimensions (Performance and Relating Responsibly) is a necessary part of good governance because governance, properly construed, cannot be just about mitigating risks, about avoiding the pain of lack of compliance with regulatory authorities (Conformance). Managing negative risks is not enough. No business would survive that had as its sole governance focus the avoidance of risk and pain. What every business must do is move toward gain (Performance) in financial and other relevant dimensions, while conducting itself in such a way that good relations (Relating Responsibly) with relevant stakeholders are maintained.

The sections that follow further outline the three dimensions of the CPR framework.

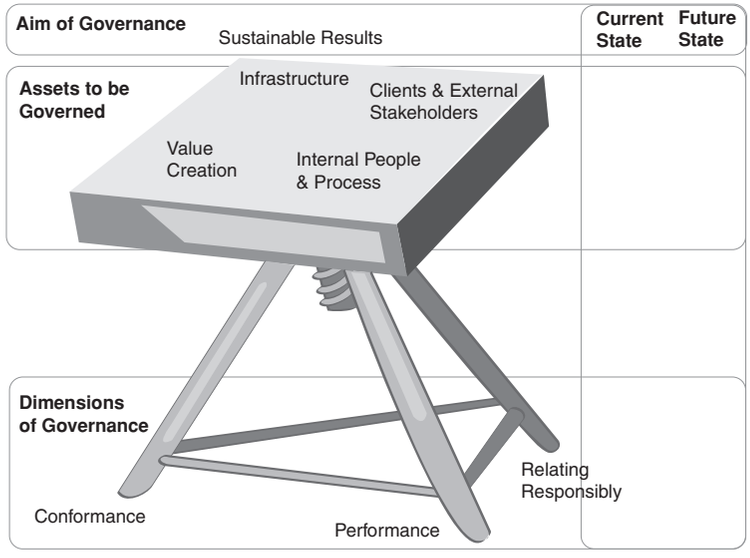

Figure 19.3 The CPR governance framework: conformance, performance, relating responsibly.

Conformance

Conformance is about ensuring compliance with relevant authorities as a means of minimizing risk to the business. It is about meeting the corporation's financial and other legal, contractual, and regulatory obligations. It is establishing and managing the control objectives. Conformance activities consist of documenting what you plan to do, doing it, and accumulating evidence to demonstrate that you are indeed doing it. The goal of conformance is compliance with relevant authorities. The instruments for measuring conformance results are the KPI dashboard (continuous) and the audit (periodic).

All business must conform to relevant laws, regulations, guidelines, and expectations, including:

- Financial requirements such as those put forth by the SEC and IRS
- Legal requirements, such as the Sarbanes-Oxley Act
- Health and safety regulations such as HIPAA and the Clean Air Protection Act
- Market expectations of customers and professional associations, such as quality certifications and hotel ratings
- Professional codes of behavior and ethics

Theoretically, all conformance areas are mandatory, but enforcement varies. While government enforcement springs to mind when the topic of conformance is raised, the market will enforce conformance to areas relating to quality and ethics.

Performance

Performance is about ensuring efficiency and effectiveness. It is doing the right things right. The goal of performance is efficiency and effectiveness in maximizing shareholder and customer value and creating predictable, sustainable value, profit, and wealth, ensuring the long-term financial viability of the business. The instruments for measuring performance results are the KPI dashboard (continuous) and the assessment review (periodic).

All businesses must measure, monitor, and manage to performance indicators from the perspective of all relevant key stakeholders, in areas such as

- Infrastructure
- Client satisfaction, including customer fulfillment
- Product capabilities
- Employee productivity, including learning and growth
- Internal business process
- Agility in all the aforementioned areas
- Business value, including the all-important financials

As you can see, these areas extend further the balanced scorecard idea of governing beyond financial performance indicators as a means to sustainable results.

Relating Responsibly

Relating Responsibly is about ensuring that the business relates to relevant stakeholders in a consistent and responsible way. It covers social values and standards, providing transparent performance statistics, demonstrating integrity, and balancing the interests of stakeholders, including

- Meeting professional, social, and ethical responsibility
- Delivering on commitment to values
- Providing transparent, timely, accurate disclosure of information regarding financial situation, performance, ownership and governance of the company; it is important to note that this aspect is not intended to duplicate the Conformance dimension—the focus here is on *how* conformance is done, rather than *what* is done, and whether or not the "how" enables or disables key relationships
- Demonstrating integrity, accountability, and fairness to, and balancing the interests of, owners, shareholders, and relevant stakeholders, including regulatory authorities
- Managing perception as well as the reality

It is about ensuring that how you do things (the means) is welcomed, rather than rejected, by relevant stakeholders. The goal of relating responsibly is stakeholder satisficing (where *satisficing* is defined as

"good enough and just a little bit better"), meaning that good relations exist with relevant stakeholders. The instruments for measuring relating responsibly results are the KPI dashboard (continuous) and the survey (periodic), which entails asking key stakeholders about their perceptions of the firm and its offerings.

All businesses must relate responsibly with relevant stakeholders such as those in Table 19.2.

Table 19.2 Typical Stakeholders of a Corporation

Stock owners	**Partners**
The board	Contract staff
Executive management	Customers
Management	Industry bodies
Employees	Consumers
Suppliers	Interest groups
Partners	Industry analysts
The press	Industry associations

Ensuring a focus on relating responsibly also acknowledges that, as pointed out in the CIMA Discussion Paper on Enterprise Governance, "…with strategic alliances, joint ventures, etc., the single-company view of corporate governance is too narrow." In other words, while it is vital to do so, it is not enough to relate responsibly with clients and shareholders, those stakeholders "internal" to the company. Relationships throughout the firm's "value constellation" must be governed.

Maintaining rapport with key stakeholders is as vital as how you get results and ultimately affects the results you get. Unidentified stakeholders and unmanaged stakeholder relationships represent a significant risk to the business. In the words of Guy Kawasaki, author and columnist for *Forbes* magazine, "good reality" is necessary. However good reality—the actual, objective situation and performance—while necessary, is not sufficient for sustainable results: good perception by key stakeholders is also necessary. Ensuring good perception requires

the systems and shrewdness of the politician, not just the technician. As Danny Maco (2003) states in *CIO Wisdom*,

> politics by definition is the art or science of governance.… Politicians, if nothing else, understand the importance of relationships as the means of getting things done within an organization.

CPR: Toward a Common Communications Channel and Protocol for Governance

The three governance dimensions—conformance, performance, and relating responsibly—are like two-way radio channels. The board and each corporate department simultaneously monitor, transmit, and receive on all three channels. For example, the board might

- Request a report from manufacturing to monitor status on environmental compliance.
- Transmit a request to engineering to map projected product development in a context of fiscal performance against the corporate business plan.
- Receive a description from IT describing the value it brings to the corporation in terms of the services it provides to corporate departments.

The point of this illustration is that no department should have a private communications link with the board with its own protocol, terminology, and timing. All departments must communicate along a standard interface with a standard protocol using standard terminology to avoid the creation of unnecessary risk and inefficiencies. All departments must strive to describe their activities with the same business-oriented, goal-based vocabulary. In all cases, the board should reasonably expect to receive timely, descriptive, and jargon-free replies.

Applying the CPR Framework to IT Governance

As stated in the introduction to the chapter, IT governance, properly construed, is a discipline within corporate governance; as such, the

board's perspective should be primary, and the board should be the ultimate driver of IT governance. As a discipline within corporate governance, IT governance activity should be directed in the dimensions important to corporate governance: CPR. This section provides guidance on how to implement the CPR framework for IT governance.

Applying the CPR framework to IT governance has a number of important implications, many of which flow down from the overarching discipline of corporate governance:

1. The board, not the IT function, must be the prime driver for IT governance and must provide a framework for governance to provide a standardized communication interface and channel for governance along with simple rules to align and inform everyday decisions and actions toward sustainable financial results.
2. As with the corporation as a whole, sustained financial results must be the objective and prime driver for IT decisions and actions.
3. Govern four assets with the purview of IT governance (infrastructure, clients and external stakeholders, internal people and process (including suppliers and partners), and value creation) in the three dimensions of CPR, and governance must include managing the current and propelling toward the future state of the enterprise.
4. Since governance is behavior, emphasis in implementing this framework must be on changing behavior rather than introducing or changing work artifacts; roles must be set out, including expected behavior changes, not just for the board and top management, but for auditors (IT, security, financial), internal staff, and external entities (such as suppliers).
5. Other IT governance activities (such as IT service continuity management) and frameworks (such as the IT Infrastructure Library) must be aligned within the CPR framework, including program office, project, financial/investment processes, service-level management, business/IT alignment, security and IT audit/conformance, and IT service management processes.

These implications lead to a set of five imperatives for governance, shown in Table 19.3.

Table 19.3 Five Imperatives for Implementing IT Governance

Ensure the board drives governance and provides the governance framework.
Focus on sustained financial results.
Govern four assets—infrastructure, clients and external stakeholders, internal people and process, value creation—in three dimensions—conformance, performance, and relating responsibly—and include within governance managing the current and directing toward the future state of the firm.
Organize around governance as behavior involving key stakeholders.
Align sources of guidance for all IT governance within the CPR framework.

The sections that follow highlight how to go about applying the CPR framework to the IT function by suggesting how to implement governance measures to meet each of the five imperatives. The five imperatives are addressed in turn.

Ensure the Board Drives Governance and Provides the Governance Framework

Governance is an activity performed jointly by the board and corporate departments. The board sets direction and policy, and departments execute and contribute their best advice and judgment. The IT function cannot be an exception. Where IT really matters to the corporation's future, it makes sense to involve corporate directors in infrastructure concerns. The following statements, from a recent article by Thomas Hoffman (2004) attest to this fact.

> A small number of companies, including Novell, Inc., and FedEx Corp., have elevated responsibility for IT governance to their boards of directors in an attempt to ensure that they have high-level oversight of technology investments.
>
> Novell's oversight committee, which also includes four other directors from outside the company, monitors major projects and decisions about Novell's technology architecture.

> FedEx created an IT oversight committee four years ago that includes board members. Like Novell's committee, the one at FedEx oversees major IT-related projects and architecture decisions and advises both the senior IT management team and other board members on technology issues, according to a spokeswoman for the Memphis-based company.

While the board should rightly drive IT governance, this does not mean that you, the CIO, cannot or should not work to influence how they go about it. In fact, you must ensure that you have what you need to be successful in your role. This starts with understanding your board's current posture, that is, the role they play in the corporation. Typical board postures include

- Window dressing (provide image enhancement)
- Strategic (address long-term and policy issues)
- Operational (direct day-to-day activities)
- Networking (create and enhance relationships)
- All-purpose (work at all levels to some extent)

Understanding your board's current posture is essential because you may need to take steps to make the integration of corporate and IT governance a "real and present" concern for your board.

Reckoning your board's current posture or raison d' être is a vital first step to understanding what you can do to influence their perception. This is essential to getting the m to drive IT governance, as they must see it as a real and present concern in order to do so.

Once you have taken into account the current posture of the board, you must decide where responsibility for IT governance should reside. You will need to define the roles and relationships relative to IT governance of key stakeholders, including owners/shareholders, the board, and top management. The following is intended as a helpful guideline for dividing these responsibilities in a large enterprise:

- Performance aspect: the board
- Conformance aspect: corporate governance committee, compliance committee, audit committee
- Relate responsibly: the board and committees

It is important to map these roles specifically to the IT function to ensure clarity of purpose and completeness of coverage.

You may also have to adjust the board's tasks, roles, and education to ensure that the integration of corporate and IT governance "takes." Ask, Do you have someone on board who has

- primary responsibility for IT governance, including in their role and responsibilities?
- the requisite specialized knowledge and expertise to do the job?
- the interest to invest the appropriate time and energy required to make a difference?

If not, consider including an outside director for this role.

Also, ask yourself the following questions:

- Do you have an independent audit, corporate governance, or compliance committee?
- Are members clear on their role in crisis management for major IT incidents, including how they should liaison with operational IT crisis teams? Have they been trained to do so?
- Is the intersection of IT and corporate governance part of your ongoing education program plan for your directors and part of your orientation program for new directors
- Is IT governance information part of the package prepared for new board members?

So far, the tactics mentioned for getting the board to drive IT governance have been largely influence, education, and role specification. Another key tactic is to leverage Service Level Management as the "communications interface" between corporate and IT governance. This tactic is outlined in the paragraphs that follow.

Leverage Service-Level Management as Nexus between IT and Corporate Governance

Properly construed, IT organizations are service providers within the corporation. Ideally, they provide a defined set of IT-based services to business customers (those who shape and fund the services) and users

(those who rely on the services to perform their work). The notion of IT as a service provider is the essence of the concept of IT service management (ITSM). ITSM is a model for managing IT as a business, where the quality of service, as perceived by the customer, is the number one driving and aligning force in the organization.

ITSM guidance includes the Service Level Management (SLM) process, which consists of the following activities:

- Defining and agreeing to the services provided (quality, service levels, cost)
- Aligning IT infrastructure provider activities to deliver on commitments
- Managing the service experience
- Managing customer–provider (and provider–provider) relationships
- Improving service levels and value within cost constraints
- Delivering as agreed, consistently maintaining commitments

The benefits of SLM include:

- Enhanced understanding by the business and IT of each others' requirements and constraints
- Better information for IT and business decision making
- Better alignment between the business and IT
- More focused and accountable providers and suppliers
- Clearly defined services, cost, and value
- Continuous improvement of services and lower costs
- Enhanced customer and provider satisfaction
- More effective business use of IT

Service-level management is the primary mechanism for managing the IT function as a services business. As shown in Figure 19.4, a good deal of effort goes into ensuring that the services IT provides meet business needs, are delivered in a way that creates and maintains customers' satisfaction, and ultimately help the corporation create value and drive profit.

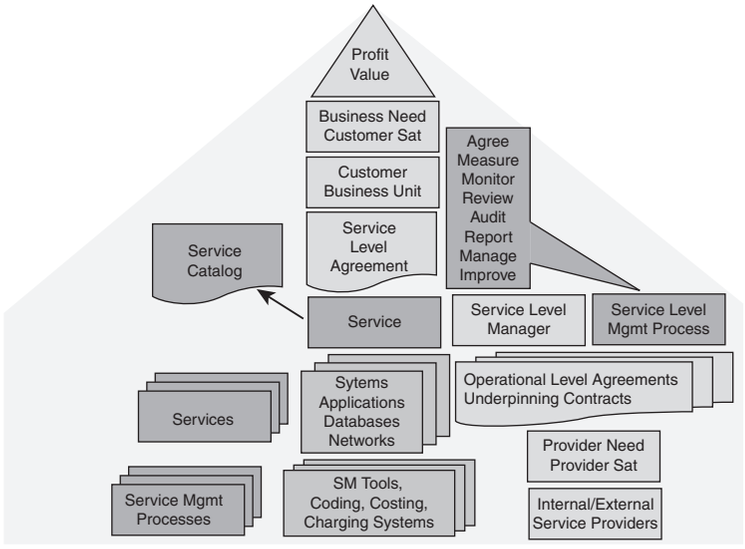

Figure 19.4 The service-level management pyramid.
Source: Pultorak, David. Exploring the Intersection of Service Level Management and Corporate Governance. BetterManagement.com Web Seminar, Thursday, December 4, 2003.

As you can see, in managing IT as a services business, services are at the center of all activity. To ensure services are delivered and supported according to commitments, the underlying technical infrastructure and systems must be up to the task. The boxes on the left-hand side of the diagram depict services as part of a larger catalog of services and may depend on other services as well as on service support and delivery processes for proper functioning. The boxes on the right-hand side illustrate that services need tending—a service manager of some sort—and rely on internal agreements between organizational units (operational level agreements) as well as contractual agreements with suppliers (underpinning contracts) to function properly. The relationship with providers needs tending, including both internal and external service providers.

The right-hand upper boxes show that a service-level management process—a process that ensures services are designed, developed, delivered, and supported as they should be through agreeing, measuring, monitoring, reviewing, auditing, reporting, managing, and improving—

must be in place to ensure consistent results and value. Lastly, the boxes at the top of the diagram show that the service-level agreement (SLA) is the primary interface to the customer, existing only to meet business needs that drive value and financial results.

Service-level management provides an ideal basis for the interface between IT and corporate governance because it and corporate governance have much in common; both service-level management and corporate governance

- Are governance mechanisms.
- Have the aspect of agency/representation; that is, a small group of individuals represents the interests of a larger group.
- Have a "down and in" management aspect and an "up and out" leadership aspect—in other words, both SLM and corporate governance require managing infrastructure and internal people and process as well as managing clients and external stakeholders.
- Focus on performance, conformance, and relating responsibly to stakeholders.
- Focus on maximizing value and minimizing risk.
- Have stakeholders in common.
- Are evolving areas after many years without change.
- Feature widespread agreement on "why" and "what" and just as widespread lack of agreement on the "how" of implementation.

How to Integrate Service-Level Management and Corporate Governance

To leverage SLM as the nexus for IT and corporate governance, it helps to start by adopting and adapting internationally recognized standards that are understood by IT. The de facto international standard for IT service management is the IT Infrastructure Library (ITIL), an open standard developed by a consortium of industry experts. ITIL includes the service-level management process and is an excellent place to start. While ITIL guidance is strong in the areas of performance and relating responsibly, it is weak in conformance aspects. To cover these, one should look to the internationally recognized guidance contained in

CobiT, which is also internationally recognized guidance, in this case focusing on control and compliance. A standards-based approach leveraging ITIL and CobiT helps ensure a defensible compliance position and accelerates compliance. A word of warning: while CobiT and ITIL can and should be used in conjunction, one should not expect them to fit together like so many jigsaw puzzle pieces; for example, a key difference is that CobiT tends to focus on describing where you should be, whereas ITIL has more coverage of how you might get there.

Focus on Sustained Financial Results

To drive governance down into the IT organization, all day-to-day decisions and actions must include a focus on and consideration of sustained financial results as a goal. For example, a "go/no-go" decision on an IT change should not be made just on technical merits; the business impact of the change must be considered as well.

Maintaining focus on financial results is another area where utilizing industry-standard ITIL guidance is extremely useful. ITIL includes process guidance for Service Level Management, as previously mentioned, which ensures a focus on the business value of services, as well as guidance for Financial Management for IT Services, which covers aspects of investment appraisal, budgeting and accounting, and charging.

Govern four assets—infrastructure, clients & external stakeholders, internal people & process, value creation—in three dimensions—conformance, performance, and relating responsibly, and include within governance managing the current and directing toward the future state of the firm

Table 19.4 outlines the dashboard of metrics required to manage the current state of the IT function and its future state along the dimensions of CPR and in the four key areas all businesses must pay attention to: infrastructure, clients and external stakeholders, internal people and process, and value creation. The idea is that a short list of the most relevant metrics for the organization be represented in each of the boxes and measured and managed to, ensuring that the IT function is driving toward sustainable financial results.

Table 19.4 CPR Key Performance Indicator Dashboard

Asset Areas _		Infrastructure		Clients & External Stakeholders		Internal People & Process		Value Creation	
Governance Dimensions_	State_	Current	Future	Current	Future	Current	Future	Current	Future
Conformance									
Performance									
Relating Responsibly									

Organize Around Governance as Behavior Involving Key Stakeholders

Each internal key stakeholder must have his or her activities relative to IT governance stated as a set of job parts and standards (completing the statement "performance is effective when…"). Figure 19.5 is adapted

4-S Job Planning

It helps to think about what we should be doing in a structured way at the start of a job, or at least annually. This technique is about that. It is called the 4-S technique because it covers Services, Stakeholders, Standards, and SMART goals. Here is how to do it:

Get out a legal pad and write for 20 minutes. Just write down what you do. Do not edit. "I answer the phone." "I analyze trouble tickets and write reports." "I do shift turnover, etc. etc." Then sort the items on the list into a set of services. For example, the items cited just now could go into a service category called. "Communication." These service categories constitute the major parts of the job. Then take each item that you wrote down ("I answer the phone") and restate it as a service by having it complete the statement, "performance is effective when…" (For example, "I answer the phone within 3 rings, and I am helpful more often than not, and when I cannot be, I figure out how to be or ask for help so I can be.")

You then look at each item and ask, "What enablers can I build on or introduce to do this task well?" Perhaps a certain training course would help.

You can then ask, "What barriers exist to doing this task well, and what can I do to eliminate them?" Perhaps the phone system is a problem. In the end, you can add another column, "obectives" where you can list actions you can take to provide enablers and minimize or eliminate barriers to your performance.

Figure 19.5 4-S job planning.
Source: Kern, Pultorak et al., *IT People: Doing More with Less*, 2005.

from the author's chapters in *IT People: Doing More with Less* (2005), which you can refer to for a worksheet and more information about how to go about it.

A similar exercise is recommended to describe the roles of clients and external stakeholders in order to capture their roles and responsibilities, although of course such documentation would not constitute job parts and standards.

Align Sources of Guidance for IT Governance with the CPR Framework

In this section, a number of common IT governance frameworks are mentioned in turn, with guidance on how each can be aligned within the CPR framework.

ISO/IEC 17799 and BS7799-2

ISO/IEC 17799 is an international standard code of practice that constitutes best practices in information security. Security guidelines are provided in the ten areas shown in Table 19.5.

Table 19.5 The Ten Guidelines Areas of ISO/IEC 17799

Business continuity planning	**Personnel security**
System access control	Security organization
System development and maintenance	Computer and network management
Physical and environmental security	Asset classification and control
Compliance	Security policy

BS7799-2 is a complementary standard to ISO/IEC 17799, providing a model for managing and improving compliance with BS7799-2 standards. BS7799-2 is the standard that one can be certified against, while ISO/IEC 17799 is a code of practice providing guidance on the identification and implementation of controls to meet the standard.

ISO/IEC 17799 and BS7799-2 can be integrated into the CPR governance framework primarily within the conformance dimension. Tracking of improvements falls under the performance dimension, and managing perceptions around security issues falls under the relating responsibly dimension. Infrastructure and internal people and process are the two primary asset areas within which ISO/IEC 17799 and BS7799-2 fit.

CMM/CMMI and ISO/IEC 15504 (SPICE)

The original Capability Maturity Model (CMM), and subsequent integrated versions (CMMI), were created by the Software Engineering Institute (SEI) to optimize software development through a framework of continuous process improvement. CMM defines five levels of maturity of software processes: initial, repeatable, defined, managed, and optimizing. ISO/IEC 15504 (also known as SPICE) is a framework for assessment methods compatible with CMMI, the first elements of which were published in 1995.

CMM/CMMI and ISO/IEC 15504 can be integrated into the CPR governance framework primarily within the Performance dimension. Tracking of compliance to specified policies and procedures falls under the Conformance dimension. Managing perceptions around capability achievement falls under the "Relating Responsibly" dimension. The primary asset area that these maturity models fall under is Internal People and Process.

Deming, EFQM, BNQP, ISO/IEC 9000, TQM, Six Sigma

Deming, EFQM, BNQP, ISO/IEC 9000, TQM, and Six Sigma are quality management systems and methods. The management aspects of these frameworks fall primarily under the Conformance dimension. The improvement aspects fall largely under the Performance dimension. The primary asset area governed by these frameworks is Internal People & Process, although Infrastructure is also important here.

IT Governance: Weill and Ross

Weill and Ross's recent book (2004) is widely quoted as a reliable source of research on IT governance. It is research-based, describing how real

practitioners view IT governance. In it, Weill and Ross conceptualize IT governance as decision making within a decision-making framework; their consequent focus is on decision rights and accountability. The book comes from an IT perspective: your perspective, that of CIO.

Weill and Ross's work spans all asset areas to be governed, and the authors provide their own take on what those assets should be: human, financial, physical, IP, information and IT, and relationship. While the book spans all dimensions of governance as well, the focus is on a subset of governance behavior—decision making. Weill and Ross's contribution is an excellent source of guidance for realizing many, but not all, aspects of the CPR framework.

CobiT

The Control Objectives for Information and Related Technology (CobiT) framework focuses on compliance and control. The guidance comes from an IT perspective, this time from the perspective of IT auditors. CobiT (ISACA 2000) substantially strengthens the EDP audit function. It is detailed, prescriptive, and complete, and provides a standardized approach to IT accountability.

As Table 19.6 shows, CobiT provides guidance in four key areas: Planning & Organization, Acquisition & Implementation, Delivery & Support, and Monitoring.

Because CobiT focuses on control and comes from the perspective of IT audit professionals, CobiT is ideal for approaching the Conformance dimension of IT governance. While the focus is on control, CobiT is applicable beyond the Conformance dimension, with guidance in seven criteria areas:

- Effectiveness
- Efficiency
- Availability
- Integrity
- Confidentiality
- Reliability
- Compliance

Table 19.6 CobiT Provides Guidance on 34 Processes in Four Key Groups

PLANNING & ORGANIZATION	ACQUISITION & IMPLEMENTATION
Define a strategic IT plan	Identify automated solutions
Define the information architecture	Acquire and maintain application software
Determine the technology direction	Acquire and maintain technology infrastructure
Define the IT organization and relationships	Develop and maintain IT procedures
Manage the investment in IT	Install and accredit systems
Communicate management aims and direction	Managing changes
Manage human resources	
Ensure compliance with external requirements	
Assess and manage risks	
Manage projects	
Manage quality	
DELIVERY & SUPPORT	**MONITORING**
Define and manage service levels	Monitor the processes
Manage third-party services	Assess internal control adequacy
Manage performance and capacity	Obtain independent assurance
Ensure continuous service	Provide for independent audit
Ensure systems security	
Identify and allocate costs	
Educate and train users	
Assist and advise IT customers	
Manage the configuration	
Manage problems and incidents	
Manage data	
Manage facilities	
Manage operations	

The primary asset area aligning with CobiT is Internal People & Process, with emphasis also in the Infrastructure asset area.

ITIL

ITIL (the Information Technology Infrastructure Library) is a collection of best practices for IT service management. ITIL's guidance is written from the perspective of the IT professional and is aimed at alignment with the business and focused on efficient and effective IT services. ITIL has been developed and widely implemented globally over the last 20 years. ITIL is appropriate for all corporations because it is vendor-neutral, nonpropriety, and scalable. That is, no matter how large or small your corporation, national or international in scope, ITIL "fits" with whatever technology you have put in place. Over 10,000 companies are using ITIL, and over 100,000 IT professionals worldwide are certified in ITIL practices.

The focus in ITIL is on effective and efficient IT processes (such as Change Management and Capacity Management) in support of the delivery of IT services. The objective is to position IT as a service provider, a partner with the business, and an enabler of business goals rather than as a mere operator of increasingly complex technology.

ITIL provides guidance and mechanisms that are ideal for realizing the performance and relating responsibly dimensions of IT governance. While the primary asset area that aligns with ITIL is internal people and process, ITIL guidance spans all four asset areas. In addition, while ITIL guidance is not focused on conformance, it enables conformance by specifying the process domains required to carry out the business of IT, which is a necessary basis for ensuring compliance with codes produced by relevant authorities (for example, a particular conformance area such as Sarbanes-Oxley compliance may require that change management processes be in place; ITIL provides the general outlines of such processes, into which controls can be inserted to ensure compliance). As such, it provides an ideal complement to CobiT as the basis for realizing full coverage in all three dimensions of governance: conformance, performance, and relating responsibly.

As such, IT must broadcast its contribution to the corporation in service terms. Who, what, where, why, and when has IT applied the resources at its command to support the business? Running an

infrastructure, no matter how complex, does not add value to customers and profit to the corporation. Aligning that infrastructure engine so that it drives toward understandable business results is the goal, and this alignment can only come about through ongoing, specific dialogue between IT and the business on the subject of service.

The focus in ITIL is on effective and efficient IT processes (change management and capacity management, etc.) and tools (service-level agreements and configuration management databases) in support of the delivery of IT services.

ITIL is very clear on what needs to be done for IT to support a business service. In focusing on business and IT alignment, it drives home the performance and relating responsibly tenets of governance through close definition of a set of processes. These processes are directed at IT customers (i.e., corporate departments that define and commission IT services) as well as users (i.e., employees that use IT day-in and day-out). The ITIL service management processes and their aims are listed and described in Table 19.7.

These ten disciplines work in concert to present the power of the underlying IT infrastructure in ways understandable to the business. Principal among its tools are the service catalog and corresponding service-level agreements (SLA) that document the mutual expectations of IT and the business. According to Weill and Ross (2004), the service catalog and SLAs…

> list available services, alternative quality levels, and related costs. Through negotiations between the IT services unit and the business units, an SLA leads to articulation of the services IT offers and the costs of the services. These negotiations clarify the requirements of the business units, thereby informing governance decisions on infrastructure, architecture, and business application needs. (p. 101)

The service catalog and SLAs drive all of the other ITIL processes. The service catalog acts a menu, and the SLA as an agreed "order" from that menu, forming the basis for common ground between corporate departments and IT. It establishes the boundaries of conformance because it has the business and IT work together to plan what to do, to do it, and to accumulate evidence that it has been done. It records the

Table 19.7 Information Technology Infrastructure Library

Corporate Departments as IT Customers (Service Delivery)		**Fellow Employees as IT Users (Service Support)**	
Process	**Aim**	**Process**	**Aim**
Service-Level Management	Agree, maintain, and where necessary improve IT service in line with business need	Incident Management	Restore normal service operation as quickly as possible or agreed
Financial Management for IT Services	Provide cost-effective stewardship of the IT investments and the financial resources used in providing IT services	Problem Management	Minimize the adverse business impact of incidents and problems
Capacity Management	Ensure that all current and future business capacity and performance aspects are supported by appropriate and cost-effective IT resources	Configuration Management	Maintain a logical picture of the IT infrastructure, including relationships among the components that constitute the infrastructure
IT Service Continuity Management	Support overall business continuity management by planning recovery of the required IT technical and services facilities	Change Management	Ensure standardized methods and procedures are used for efficient and prompt handling of all changes
Availability Management	Optimize the availability of the IT infrastructure and supporting organization	Release Management	Release new or revised IT services where both technical and nontechnical aspects are considered together

Source: Process definitions abridged from van Bon, Pieper, and van der Veen (2004)

mutual understanding of quality whose measurement brings performance characteristics to the fore. Lastly, it sets the cost parameters—what the business can afford and what IT can spend—reflecting the balance of supply and demand that underscores relating responsibly.

IT service management is not a one-step approach for infusing IT with the three-part framework of governance, but it takes the first step by elevating the dialogue where business goals and objectives are the nouns, service is the verb, and the innumerable details that constitute the technical infrastructure are secondary.

In short, the service focus proposed here allows the board to expect more, to demand more, and to require greater transparency in reporting on the business value of IT services. Microsoft adopted and adapted ITIL, transforming it into the Microsoft Operations Framework (MOF) to secure even stronger benefits for the corporation and its goals. As Ron Markezich, CIO for Microsoft Corporation says, "Our goal in IT at Microsoft is to use technology as a competitive advantage for Microsoft. Our focus on Microsoft Operations Framework and service management helps us ensure a foundation of reliable, effective and trustworthy IT services that are required for our users to get the most out of the services IT provides."

Other Mechanisms Associated with IT Governance

Some professionals equate IT governance in whole or in part with a variety of management mechanisms in use in organizations. Chief among them are program, project, and portfolio management, enterprise architecture, business and IT alignment, and the strategy, policy-setting, and planning functions performed by the board, executive management, and specialized staff. A variety of guidance exists for these mechanisms, such as the PMBOK for project management. While it is beyond the scope of this chapter to review all such guidance, it is important to note that many consider such mechanisms an important part, and in some cases, the primary part of IT governance, sometimes going so far as equating these mechanisms with governance. While each has a role in governance, the general guidance given here is to apply such mechanisms within an overarching framework that aligns them.

Call to Action

Governance requires action. In fact, governance *is* action, equivalent to the sum of the behaviors that guide relationships between and among corporations and their constitute parts. While governance can sometimes be viewed as formal rules and procedures, there are things you as CIO can do tomorrow to shape your board's view of IT governance. Some ideas for how to proceed follow:

- Suggest a discussion on governance be placed on the board agenda to gain concurrence on your board's thinking on the matter.
- Have the wider definition of governance broadcast throughout the corporation.
- Suggest that the wider definition of governance filter out to key customers and suppliers.
- Arrange joint IT–company management discussions on vital business drivers to further business and IT alignment.
- Start working with selected corporate departments (finance, manufacturing, sales, etc.) to start the process of ascertaining the business value of IT services, conducting a business impact analysis and initial service-level agreement discussions.
- Secure an invitation to a meeting of the board of directors to report on the effectiveness of service-level agreements already in place within the corporation.
- Join in discussions with fellow CIOs on the contribution governance makes to customer value and company profit.

In the end, governance is strongly oriented toward sustainability: ensuring that the corporation is successful today and positioned for tomorrow. Corporate governance, including IT governance, is simultaneously the scout and sentry on the frontier of company growth.

IT Governance Checklist

Conformance

1. Do you have and follow a formal risk management process to evaluate the technical and business advantages and disadvantages accompanying infrastructure projects?
2. What listening posts have you established to understand the nature of new regulatory or legal requirements that are being considered applicable to your industry?
3. Have you charted the IT infrastructure implications of the result of the three recent major marketing initiatives your corporation has launched? Are there ways you should "tie in" to such initiatives to anticipate the IT impact?
4. Which industry-specific codes of behavior and ethics influence the operation of the IT functions within your corporation? How are you accumulating evidence that you support such codes?
5. Have recent EDP audit findings and recommendations been addressed as part of the day-to-day practice in your area?

Performance

1. Are you satisfied with the mechanisms you have in place for measuring and reporting the cost of IT services to the business? Have you analyzed those costs in comparison to the value the business derives from these services?
2. What productivity metrics have you identified for IT staff roles and positions? Have you seen improvement in the measurements over the last quarter?
3. Since IT services support business processes, how have you and the business collaborated in continuous process improvement programs to drive additional effectiveness and efficiency?

Relating Responsibly

1. Have you identified the key internal and external stakeholders in the quality delivery of IT service? Do you have a periodic means to communicate with such stakeholders?
2. How does your IT organization "give back" to the community surrounding your installations?

3. Are your suppliers aware of your goals and objectives? Have you invited them to participate in key IT service management initiatives?
4. Does your corporate board or owners see IT acting in a leadership role in shaping governance procedures and execution?

Infrastructure

1. Has the infrastructure been engineered such that it consistently supports meeting the requirements and commitments of the business?
2. Is this infrastructure robust enough to maintain acceptable service levels to the business?
3. Has the infrastructure been designed, developed, and implemented to provide for high enough levels of availability, flexibility, scalability, and performance?
4. Is the infrastructure internally and externally secure?

Clients and External Stakeholders

1. Is there an appropriate level of customer satisfaction with the level of service?
2. Are the services provided appropriate and fit-for-purpose?
3. Is the customer experience and feedback being gathered and used in a continuous service improvement process
4. How well are the organizational culture and perception of the services provided being monitored and compared against the value proposition to the customer?

Internal People and Process

1. Are the ongoing operational activities and the investments being made to provide the necessary services being monitored?
2. Are these activities and investments being compared to the results and valued-added benefits being provided?
3. Is the offering determined as fit-to-purpose based on the value provided and the cost effectiveness?
4. Does the service provided leverage and maximize the use of the organization's intellectual property?

Value Creation

1. Are there effective quality processes in place to ensure the development, delivery, and ongoing support of the IT services and infrastructure?
2. Are there processes in place to support the internal and external relationships between service providers and suppliers and their interactive performance?

References

Literary Sources: Linking Corporate and IT governance

Pultorak, D., and J. Kerrigan, 2005. "CPR: A Framework for Corporate and IT Governance." *Directors Monthly*, 29(2). February.

Pultorak, D., 2003. Exploring the Intersection of Service Level Management and Corporate Governance. *BetterManagement.com Web Seminar*, Thursday, December 4, 2003.

Pultorak, D., 2001. Yes we can do it—and this is what it will cost. *Presentation to the itSMF Annual Conference*, Brighton, UK.

Literary Sources: Corporate Governance

COSO, 1994. *IT Internal Control—Integrated Framework (COSO report)*. Committee of Sponsoring Organizations of the Treadway Commission. 151 pages. Zaltbommel, The Netherlands.

Kaplan, R. S., and D. P. Norton, 1996. *The Balanced Scorecard: Translating Strategy Into Action*. Harvard Business School Press.

Literary Sources: IT governance

Brand, K., and H. Boonen, 2004. *IT Governance: A Pocket Guide Based on COBIT®*. Van Haren Publishing.

Hoffman, T., 2004. "IT Oversight Gets Attention at Board Level." *Computerworld*. May 17.

IT Governance Institute, 2003. *Board Briefing on IT Governance* (2nd ed.). IT Governance Institute.

Information Systems Audit and Control Association (ISACA), 2000. *CoBiT Framework*. ISACA and IT Governance Institute.

Maco, D., 2003. "Governance." In Dean Lane (Editor), *CIO Wisdom*. Prentice Hall PTR, pp. 123–149.

van Bon, J., M. Pieper, and A. van der Veen, 2004. *IT Service Management: An Introduction Based on ITIL®*. Van Haren Publishing.

van Grembergen, W., 2004. *Strategies for Information Technology Governance*. Idea Group Publishing.

Weill, P., and J. W. Ross, 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press.

Weston, H. (Editor), 2001. *Service Delivery*. The Stationary Office. London, England.

Web Sources: Corporate and IT Governance

Balanced Scorecard: http://www.balancedscorecard.org

Bettermanagement.com (Exploring the Intersection of IT Service Level Management and Corporate Governance, Archived Web Seminar): http://www.bettermanagement.com/Seminars/Seminar.aspx?LibraryID=8341

CIMA Enterprise Governance: a CIMA Discussion Paper: http://www.cimaglobal.com/cps/xbcr/SID-0AAAC564-00E392AB/live/entgov_execrpt_0204.pdf

The Conference Board Inc.: http://www.conference-board.org/

EZCOBIT: http://audit.byu.edu/website/tools/COBIT/cobit.cfm

Fox IT, LLC: http://us.foxit.net/

IT Governance Institute: http://www.itgi.org/

Information Systems Audit and Control Association (ISACA): http://www.isaca.org/

Information Technology Infrastructure Library (ITIL): http://www.ogc.gov.uk/index.asp?id=2261

Information Technology Service Management Forum (itSMF): http://www.itsmf.com/

Institute of Chartered Accountants in England and Wales (ICAEW), information on corporate governance: http://www.icaew.co.uk/index.cfm?AUB=tb2i_47496,MNXI_47496

KPMG Audit Committee Institute: http://www.kpmg.com/aci/home.html

National Association of Corporate Directors: http://www.nacgonline.org/

Organization for Economic Co-operation and Development, on Corporate Governance: http://www.oecd.org/topic/0,2686,en_2649_37439_1_1_1_1_37439,00.html

Pultorak & Associates, Ltd.: http://www.pultorak.com/