

Conformance, Performance, and Rapport: A Framework for Corporate and IT Governance

By David Pultorak and Jim Kerrigan

Governance should extend out from the board in three directions: conformance, performance, and rapport (CPR). These three dimensions are 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). No business would survive that had as its sole governance focus the avoidance of risk and pain. What all businesses must do is go towards gain (performance) in financial and other relevant dimensions, while conducting itself in such a way that good relations (rapport) are maintained with relevant stakeholders.

The three-part CPR framework of governance applies to *all* parts of the corporation, because corporate departments—finance, manufacturing, marketing, sales, engineering, Information Services, etc.—must conform to relevant regulatory authorities and perform financially and in other ways, and do so in a way that maintains rapport with relevant stakeholders.

The CPR framework for governance highlights the importance of employing robust governance mechanisms. This article addresses a few such mechanisms—the balanced scorecard (BSC), CobiT (control objectives for information and related technology), and ITIL® (Information Technology Infrastructure Library)—to illustrate how one might employ them to contribute to the implementation of the three dimensions of governance. The case of the information technology (IT) function and IT

governance is used to further illustrate how the CPR framework can be employed. In so doing, we hope to extend Schumann and Chinoy's August 2004 *Directors Monthly* article on IT governance.

Corporate Governance

After years of stable development, corporate governance is receiving significant attention. Historically, there was a strong emphasis on finance. Corporate governance was virtually synonymous with the measuring, monitoring, and reporting of the financial condition of the enterprise.

But that has changed. About a decade ago it became clear that focusing on financial performance alone was not enough to ensure sustainable results. This fact was highlighted by Robert S. Kaplan and David P. Norton and summarized in their research. Kaplan and Norton recommended a “balanced scorecard” of governance dimensions, including, in addition to financial performance, business process, customer fulfillment, and learning and growth. The balanced scorecard dramatically extended the factors to be considered in corporate governance.

In the nine years since Kaplan and Norton first published their research, the number of authorities, pieces of legislation, and industry regulations and standards that corporations must comply with has increased dramatically. And many corporations have stumbled even as they worked towards a balanced scorecard of results because the way they conducted themselves “turned off” rather than “turned on” relevant stakeholders.

And while business fundamentals remain the same, the landscape upon which business is played out has changed drastically since 1996, when business use of the Internet was still in its infancy. Today, enterprises are thoroughly networked entities operating in massively networked marketplaces. A corporation's customers, competition, and colleagues are all

Director Summary: Using the governance of information technology as an example, the authors illustrate that boards should strive for regulatory conformance, financial performance, and rapport with stakeholders to provide a good governance framework.



Performance is about ensuring efficiency and effectiveness. It is doing the right things, right.

deeply interconnected. The result of a networked marketplace is an increase in both the frequency and variability of demands on the business, including opportunities and threats.

An example may help illustrate: imagine yourself as a medieval king presiding over a backward country with no good road system to speak of interconnecting its villages. You take the bold stroke of building roads interconnecting the villages. As a result of your actions, vendors now have a realistic opportunity to sell their wares in not just one market, but several markets. And highwaymen now have a realistic opportunity of robbing people on more than just one road. The end result is that by networking the villages with a system of roads, you have increased both the frequency and variability of opportunities and threats. This is precisely what has happened with our economy with the “Internet highway.” This situation creates a requirement for corporate directors to broaden the foundation of corporate governance.

The balanced scorecard provides the board and corporate management with four primary perspectives on conformance:

- **Financial.** Statistical treatment of the economic consequences of actions already taken.
- **Internal business process.** Activities that must be done well to deliver value to customers and satisfy shareholder expectations.
- **Learning and growth.** Procedures that focus on long term corporate growth and improvement.
- **Customer.** Measurement of customer satisfaction, acquisition/retention, profitability, and business volume share by market and account.

While it remains a useful tool, the BSC does not focus on the rapport and conformance dimensions of governance.

The CPR Governance Framework

A corporate entity has an obligation to meet recognized goals in an organized way with regard to a wide range of stakeholders. The CPR governance framework divides governance into three dimensions: *conformance*, *performance*, and *rapport*.

Conformance

Conformance is about ensuring compliance. It is establishing and managing the control objectives. Conformance activities consist of documenting what you plan to do, doing it, and accumulating evidence that you are doing it. The goal of conformance is compliance with relevant authorities. The instrument for measuring conformance results is the audit.

All business must conform to relevant:

- Regulatory authorities, such as the IRS and the FDA
- Legal requirements, such as the Sarbanes-Oxley Act
- Industry specific rules, such as HIPAA
- Market expectations of customers and professional associations, such as hotel ratings
- Professional codes of behavior and ethics

Some of these conformance areas are mandatory. Others are optional theoretically but necessary for business purposes—for example, while there is no legal requirement for a hotel to maintain a 3–5 star rating, customers will avoid hotels without such ratings. And while there is no legal requirement for members of an industry association to abide by its code of ethics, compliance with such codes makes good business sense.

Performance

Performance is about ensuring efficiency and effectiveness. It is doing the right things, right. The goal of performance is efficiency and effectiveness. Performance is about ensuring the predictable, sustainable creation of customer value and company profit. The instrument for measuring performance results is the assessment review.

All businesses must measure, monitor, and report on relevant performance indicators, including financial, product capabilities, employee productivity, internal business process, customer fulfillment, learning and growth, and agility.

These areas extend further the balanced scorecard idea of governing beyond financial performance indicators as a means to sustainable results.

Rapport

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

It is about ensuring how you do things (the means) “turns on” and does not “turn off” relevant stakeholders. The goal of rapport is good relations with relevant stakeholders. The instrument for measuring rapport results is the survey.



The board should reasonably expect to receive timely, descriptive, and jargon-free replies.

These three governance dimensions—conformance, performance, and rapport—are like two-way radio channels. The board and each corporate department simultaneously monitors, transmits, and receives on all three channels. For example, the board might:

- Monitor status on environmental compliance from manufacturing.
- 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.

To ensure alignment and efficiency, no department should have a private communications link with its own protocol, terminology, and timing. 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.

To illustrate the CPR governance framework, the sections that follow apply it to the issues of information technology governance.

The CPR Framework Applied to Information Technology Governance

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 information technology really matters to the corporation's future, it makes sense to involve corporate directors in infrastructure concerns.

Like corporate governance, IT governance is undergoing rapid evolution after years of inattention. Recent emphasis has been on the two primary standards for IT governance: CobiT and ITIL.

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. It is detailed,

prescriptive, and complete, and provides a standardized approach to IT accountability.

CobiT provides a durable structure for IT auditors to approach the conformance issues of governance. It groups processes into four domains:

- Planning and organization. Strategy and tactics for IT to contribute to business objectives.
- Acquisition and implementation. Identify IT solutions, developed or acquired, implemented and integrated.
- Delivery and support. Creation and delivery of necessary support services.
- Monitoring. Periodic, regular assessment of IT processes for quality and compliance.

CobiT's strength is conformance but more coverage is needed for governance in the areas of performance and rapport.

ITIL[®]

The Information Technology Infrastructure Library (ITIL) is a collection of best practices for IT service management. ITIL's guidance is written from the perspective of the IT professional, aimed at alignment with the business, and focused on efficient and effective IT services. ITIL is and has been developed and widely implemented globally over the last 20 years. ITIL is appropriate for corporations because it is vendor neutral, non-proprietary 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.

ITIL provides guidance and mechanisms for managing performance and rapport. While ITIL is not focused on conformance, it enables it by specifying the management domains required to carry out the business of IT, which is a necessary basis for ensuring compliance with codes produced by relevant authorities. Together, CobiT and ITIL are a powerful combination addressing each dimension of governance: conformance, performance, and rapport.

ITIL is a service management framework, and services are the heart of IT service management. Service management is organizing around services—not technology or the customer by themselves. It is a powerful concept to guide the use of information technology. It allows IT to align and synchronize with the business mission of the corporation and satisfy internal customers rather than concentrate on technology issues.

In service management, IT has an essential role: enterprise service provider. The corporation's expectation of IT is based on services, not technology. That is, IT delivers services to the corporation that *result* from the management



of an underlying computer and network infrastructure. IT's contribution is not the *operation* of that infrastructure, it is using that infrastructure to create and deliver services for enduring business value.

Each individual ITIL process has a specific aim. For example, ITIL calls the process dedicated to improving business and IT alignment "Service Level Management," and the process for helping users get back to work again after a system failure "Incident Management," etc. Such a document drives all of the other ITIL processes. Like a menu or a set of specifications, it is the 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, do it, and accumulate evidence that it has been done. It records the mutual understanding of quality whose measurement brings *performance* characteristics to the fore. Lastly, it sets the cost parameters — what the business can afford and IT can spend — reflecting the balance of supply and demand the underscores *rapport*.

IT service management is not a cure-all 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 all the gory details that constitute the technical infrastructure are secondary.

Guidance for Boards on Effective Governance over Information Technology

While boards have traditionally reviewed business strategy and strategic risks, few boards have focused on IT, despite the large investments and vast risks. This divide may exist because IT requires deeper technical insight than other disciplines. Generally, board members have expertise in areas other than IT, and it has not always been made clear to the board how IT enables the enterprise and creates risks and opportunities. IT has been traditionally treated as an extended member of the corporate family—related to, but somewhat separated from, the core business. IT is also complex, especially in globally extended enterprises operating in a networked model.

Board Role in IT Governance

To ensure IT governance initiatives are focused on the most effective areas, the board should ensure an effective action plan is developed and followed. With the goal of taking appropriate ownership of IT governance and setting management direction, a board should:

- Ensure IT is on its agenda.
- Challenge management's activities regarding IT so IT issues are uncovered.
- Guide management in aligning IT initiatives with real business needs.
- Insist that IT performance be measured and reported to the board.
- Consider establishing an IT strategy

committee with responsibility for communicating IT issues between board and management.

- Insist that management implement a framework for IT governance, such as control objectives for information and related technology (CobIT).

Top management issues for the oversight of IT have moved from technology to management-related arenas. These issues clearly map to the IT governance areas of strategic alignment, value delivery, risk management, resource management, and performance measurement. A board's role in these areas focuses on the following responsibilities.

Strategic alignment. Boards should ensure management has put in place an effective strategic planning process, ratify the aligned business and IT strategy, and ensure the IT organizational structure complements the business model and direction.

Value delivery. Boards should ascertain that management has put processes and practices in place that enable IT to deliver provable value to the business, and ensure IT investments represent a balance of risk and benefit, with acceptable budgets.

IT resource management. Boards should monitor how management determines the resources needed to achieve strategic goals, and ensure a proper balance of IT investments for sustaining and growing the enterprise.

Risk management. Boards should be aware of IT risk exposures and their containment, and evaluate the effectiveness of management's monitoring of IT risks.

Performance management. Boards should assess senior management's performance on IT strategies in operation, and work with executives to define and monitor high-level IT performance.

An effective IT governance framework will help boards understand the issues and strategic importance of IT. It will also assist in ensuring that the enterprise can sustain its operations and implement the strategies required to continue its business into the future. The framework also provides assurance to the board that expectations for IT are met and IT risks are addressed.

Because IT is an integral part of the business, boards need to ensure that IT governance is an integral part of their governance over the entire enterprise.

Michael P. Cangemi is former president and CEO of Etienne Aigner Group, Inc., and past president of the Information Systems Audit and Control Association (ISACA). He has been editor-in-chief of the *Information Systems Control Journal* since 1987. For more information, visit <http://accounting.rutgers.edu/raw/isaca/cangemi/>.

The guidance contained in CobiT are certainly significant tools and contributions to the industry and focus on conformance. ITIL champions efficiency and effectiveness, and relating responsibly with relevant stakeholders; while it enables control and compliance, it does not focus there. One should begin to see that using CobiT and ITIL together forms the basis for a more complete IT governance mechanism.

Each of the bodies of work cited above comes from the perspective of IT, and not that of the corporate board. The CPR framework is proposed as the basis for a governance framework that:

- Describes the key dimensions of governance: conformance, performance, and rapport.
- Ensures complete coverage of key indicators of sustained business results.
- Is compatible with prescriptive, function-specific governance mechanisms like ITIL and CobiT.

Call to Action

Governance requires action. It suggests behaviors to 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 can you do tomorrow to shape your board's view of IT governance:

- 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.
- Propose that the wider definition of governance filter out to key customers and suppliers.
- Ask company management to discuss vital business drivers with IT management to further business and IT alignment.
- Invite IT management to report on the effectiveness of service level agreements already in place within the corporation.
- Seek support from NACD for white papers and training on governance in the large and IT governance in particular.

In the long run, governance is strongly oriented towards 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. ■

David Pultorak is president of Fox IT, LLC, and CEO of Pultorak & Associates. **Jim Kerrigan** is senior manager at Fox IT. Both have served on private and nonprofit boards.

NEW CORPORATE BOARD MEMBERS

ADESA, Inc. Carmel, IN

David G. Gartzke,
Chairman

Thomas L.

Cunningham
Brenda Flayton
Dennis O. Green
George J. Lawrence
Angel Rodolfo Sales
Nick Smith
W. Van Bussmann
Donald C. Wegmiller
Deborah L. Weinstein

Blue Cross Blue Shield-Kansas City Kansas City, MO

Tom Bowser, President
& CEO

David R. Bywaters
Melvin L. Glazer, MD
Anita B. Gorman
Karon Harris Hicks
Rick Kastner
Garry K. Kemp
Janice C. Kreamer
Ben D. McCallister, MD
Travis D.L. Newsome
L. Keith Querry
Sam R. Reda
James R. Roath
Larry A. Rues, MD
Danley K. Sheldon

Capital District Physicians' Health Plan

Albany, NY

John D. Bennett, M.D.,
Chairman
William Cromie, M.D.,
President & CEO

J. Michael Brennan
Peter T. Burkart, M.D.
M. Bruce Cohen
Gennaro A. Daniels,
M.D.
Barbara Downs
Robert H. Dropkin,
M.D.
Daniel Frasca
Robert C. Griffin
Douglas P. Larsen, D.O.
James C. Leyhane,
M.D.
Kelly A. Lovell
William M. Notis, M.D.
Martha H. Pofit
Stuart A. Rosenberg,
M.D.
Stephen C. Simmons

Cell Therapeutics, Inc.

Seattle, WA

James Bianco,
Founder, President &
CEO

John Fluke
Vartan Gregorian
Richard Leigh
Max Link
Phillip M. Nudelman
Mary Munding

Erich Platzer
Jack Singer
Silvano Spinelli

Insight Enterprises, Inc. Tempe, AZ

Timothy A. Crown,
Chairman
Eric J. Crown,
Chairman Emeritus

Bennett Dorrance
Michael M. Fisher
Larry A. Gunning
Robertson C. Jones
Stanley Laybourne
Mark Rogers

Johnson Controls, Inc. Milwaukee, WI

John M. Barth,
President & CEO

Dennis W. Archer
Robert L. Barnett
Natalie A. Black
Paul A. Brunner
Robert A. Cornog
Willie D. Davis
Jeffrey A. Joerres
William H. Lacy
Southwood J. Morcott
Jerome D. Okarma
Steven A. Roell
Richard F. Teerlink

North American Scientific, Inc. Chatsworth, CA

Michael Cutrer,
President & CEO
Irwin Gruverman,
Chairman

Donald N. Ecker
John Friede
Jonathan Gertler
David King
John W. Manzetti
Mitchell Saranow
Gary Wilner
Mancy Wysenski

OGE Energy Corporation Oklahoma City, OK

Steven E. Moore,
Chairman, President
& CEO

Carla D. Brockman
Herbert H. Champlin
Luke Corbett
William E. Durrett
Martha Griffin
John D. Groendyke
Robert Kelley
Linda Petree Lambert
Ronald H. White
J.D. Williams

O.I. Corporation College Station, TX

William Botts,
President, CEO, &
Chariman

Jack S. Anderson
Richard W. K.
Chapman
Edwin B. King
Craig R. Whited

Pfizer, Inc. New York, NY

Henry A. McKinnell,
Chairman & CEO
William C. Steere,
Chairman Emeritus

Michael S. Brown
M. Anthony Burns
Robert N. Burt
W. Don Cornwell
Margaret Foran
William H. Gray, III
Constance J. Horner
William R. Howell
Stanley O. Ikenberry
George A. Lorch
Jeffrey B. Kinder
John L. LaMattina
Dana G. Mead
Franklin D. Raines
D. L. Shedlarz
Ruth J. Simmons
Jean-Paul Valles

Semtech Corporation Camarillo, CA

Jason L. Carlson,
President & CEO
John D. Poe, Chairman

Glen M. Antle
James P. Burra
Rockell N. Hankin
James T. Lindstrom
John L. Piotrowski
James T. Schraith

Sprint Corporation Overland Park, KS

Gary D. Forsee,
Chairman & CEO
DuBose Ausley
Gordon M. Bethume
E. Linn Draper, Jr.
Deborah A. Henretta
Irvine O. Hockaday
Linda Koch Lorimer
Charles E. Rice
Louis W. Smith
Gerald L. Storch
William H. Swanson

The Williams Companies, Inc. Tulsa, OK

Steven J. Malcolm,
President, Chairman
& CEO

Hugh M. Chapman
William E. Green
Juanita H. Hinshaw
William R. Howell
Charles M. Lillis
George A. Lorch
William G. Lowrie
Frank T. MacLinnis
Janice D. Stoney
Joseph H. Williams
John H. Williams