Under Control

Governance Across the Enterprise

Jacob Lamm

Sumner Blount, Steve Boston, Marc Camm, Robert Cirabisi, Nancy E. Cooper, Dr. Galina Datskovsky, Ph.D., CRM, Christopher Fox, Kenneth V. Handal, William E. McCracken, John Meyer, Helge Scheil, Alan Srulowitz, Rob Zanella

CA PRESS

Apress®

Under Control: Governance Across the Enterprise

ISBN-13 (pbk): 978-1-4302-1592-9

ISBN-13 (electronic): 978-1-4302-1593-6

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

President and Publisher: Paul Manning
Lead Editor: Jeffrey Pepper
Contributing Editor: Lynne Mahoney
Editorial Board: Clay Andres, Steve Anglin, Mark Beckner, Ewan Buckingham, Gary Cornell, Jonathan Gennick, Jonathan Hassell, Michelle Lowman, Matthew Moodie, Duncan Parkes, Jeffrey Pepper, Frank Pohlmann, Douglas Pundick, Ben Renow-Clarke, Dominic Shakeshaft, Matt Wade, Tom Welsh
Coordinating Editor: Jim Markham
Copy Editor: Tiffany Taylor
Compositor: Apress Production
Indexer: nSight, Inc.
Artist: April Milne
Cover Designer: Anna Ishchenko

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress by e-mail info@apress.com, or visit `http://www.apress.com`.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at `http://www.apress.com/info/bulksales`.

Contents

About the Authors

Jacob Lamm is executive vice president of Strategy and Corporate Development at CA. In this role, he is responsible for coordinating the company's overall business strategy, as well as developing strategy for the selection, prioritization, and execution of acquisitions. In addition, Jacob leads CA's Business Incubation business units, which are charged with exploring opportunities to build businesses in new markets. He is also a member of CA's Executive Leadership Team, which defines and ensures execution of the Company's business and technical strategies.

Jacob has held various management positions since joining CA in 1998. Prior to assuming his current role he served as executive vice president of CA's Governance Group, a collection of business units focused on delivering solutions that help organizations effectively govern all areas of operations. Earlier, he was executive vice president and general manager of CA's Business Service Optimization business unit.

Jacob has more than 20 years of industry experience covering a wide range of technologies and business applications.

He joined CA with its acquisition of Professional Help Desk (PHD), where he was co-founder and served as executive vice president and chief technology officer. Under his leadership, PHD evolved into one of the strongest products on the market and gained industry recognition as having the most visionary service management solution.

Prior to founding PHD, Jacob served as a senior manager at Con Edison in New York, where he was responsible for integrating new technologies into the company's business systems, including wireless communications, data warehousing, imaging, and Internet solutions. A graduate of Brooklyn College, Jacob earned a bachelor's degree in computer information science.

Sumner Blount is the director of Product Marketing for the GRC business unit at CA. He is responsible for product positioning, and is a significant contributor to thought-leadership activities related to GRC. Prior to this role, he was the director of Solutions Marketing for the Security Management business unit.

Sumner joined CA from Netegrity, where he served as the senior product manager for SiteMinder for three years. Prior to Netegrity, he managed the large computer operating system development group at Digital Equipment and Prime Computer, and was director of software for Pathway Designs. He later was instrumental in the original conception and development of the DCE (Distributed Computing Environment) technology from the Open Software Foundation, and served as the DCE program manager within Digital. He has held a number of product management positions, including management of the Distributed Computing Product Management group at Digital.

His articles have appeared in several industry publications including Compliance Executive Journal, Business Management Journal and Mainframe Executive and he has spoken at a number of industry conferences.

Sumner received a Bachelor of Science degree in Math from the University of North Carolina, and a Masters degree in Computer Science from the University of Connecticut.

Steve Boston is vice president and chief sustainability officer at CA. He is responsible for CA's worldwide sustainability efforts. Steve works on various initiatives applying IT technology to foster solutions for environmental and social issues. He is currently focused on driving the development of energy management technologies.

Steve brings historical and big-picture perspectives to technical and operational issues and leverages business intelligence to expand CA's ability to positively impact our planet and communities.

During Steve's 20 year career in the IT industry, prior to joining CA, he held positions in strategy, development and management. Steve was a member of IBM's Software Group Strategy unit and led an effort to determine where Digital Media fit into IBM's overall strategy and helped to define the company's Itanium II positioning.

Steve has filed more than 25 patent applications in various emerging technology areas. He participates in CA's Technology Innovation Committee and is a member of CA's Council for Technical Excellence.

Steve serves as member of the U.S. Council for Competitiveness on the Energy, Security, Innovation and Sustainability committee. He is also a member of the World Economic Forum's Committee for Information and Communication Technology.

Steve attended Northeastern University where he majored in business.

Marc Camm is senior vice president and general manager of Governance, Risk and Compliance products at CA. He is responsible for establishing CA as a leader in the emerging GRC market.

Marc joined CA in 2003 through the acquisition of Adjoin and has since held a number of management positions. Prior to assuming his current role, he served as the vice president and general manager of CA's mobile device management business unit, which was focused on securing and managing Smartphone technology in the enterprise. Earlier, he was vice president and general manager of CA's Managed Vulnerability Service, which was the forerunner of CA's first Software as Service offering. Marc has been instrumental in conceiving, developing and expanding CA's new business opportunities.

Prior to joining CA, Marc was chief operating officer of Adjoin, responsible for marketing, sales, business development, and product management groups. A 20-year software industry veteran, Marc has held senior management positions at Microsoft, Symantec, Delrina and BindView in addition to working with several other technology startups.

Marc received a Bachelor of Commerce degree from the University of Manitoba in Canada.

Robert Cirabisi is CA's senior vice president and chief risk officer, responsible for overseeing the company's worldwide Enterprise Risk Management Function and Global Quality and Controls.

In his role as chief risk officer, Bob is responsible for examining the company's activities and establishing a framework to protect the company against significant risks, both internal and external, and to consider significant risks, trends and uncertainties arising with respect to the company's strategies, business operations, financial reporting, and legal and regulatory affairs. This role reports dually to CA's Chief Administrative Officer and to the Compliance and Risk Committee of the Board of Directors. Bob is also responsible for the prioritization and global rollout of CA's GRC Manager product across CA's various business functions.

Bob joined CA in 2000 and has held various positions including chief audit executive, corporate controller, acting chief financial officer, chief accounting officer, vice president of Investor Relations and U.S. controller.

Prior to joining CA, Bob had over 13 years of audit experience with Ernst & Young and Arthur Anderson, specializing in its energy and utility practice. Bob is a Certified Public Accountant and a graduate of Hofstra University in Hempstead NY.

Nancy E. Cooper, executive vice president and chief financial officer, is responsible for all of CA's corporate and business unit financial functions worldwide, including the controller role, treasury, tax, investor relations, and risk management. Nancy joined CA in August of 2006.

Nancy has nearly 30 years of finance experience, most recently serving as chief financial officer for IMS Health, Incorporated, a leading provider of market intelligence to the pharmaceutical and healthcare industries. There, her responsibilities included finance and accounting, treasury, investor relations, human resources, and business development. She was instrumental in integrating IMS' financial systems and finance teams representing more than 100 countries and closing 30 acquisitions IMS made during her tenure.

Prior to joining IMS Health, Nancy was the chief financial officer of Reciprocal, Inc., a leading digital rights management and consulting firm whose clients included McGraw Hill, Sony, Time Warner, and Reuters. In addition, she served as chief financial officer of Pitney Bowes Credit Corporation, an international credit company. In 1998, Nancy served as a partner responsible for finance and administration at General Atlantic Partners, a private equity firm focused on software and services investments.

From 1976 to 1998, Nancy held various positions of increasing responsibility at IBM, including CFO of the Global Industries Division, assistant corporate controller, and controller and treasurer of IBM Credit Corporation. Prior to that, she served as director of Financial Management Systems, Pricing and Financial Planning at IBM, responsible for pricing strategy and financial planning management among many IBM divisions worldwide.

Nancy holds a Bachelor of Arts degree in Economics and Political Science from Bucknell University and an MBA from the Harvard Graduate School of Business Administration.

Dr. Galina Datskovsky, Ph.D., CRM, is senior vice president and general manager of the Information Governance business unit at CA, responsible for the CA Message Manager and CA Records Manager product lines. She is also recognized as a Distinguished Engineer at CA, and joined the company in 2006 with the acquisition of MDY Group International, where she served as founder and CEO.

Prior to founding MDY, Galina consulted for IBM and Bell Labs and taught at the Fordham University Graduate School of Business and the Graduate School of Arts and Sciences at Columbia University.

Galina received her Certified Records Manager (CRM) certification in 2004 and is recognized around the world as an expert in records management and associated technologies, including the convergence of records and document management, email and physical records management, and federated records management.

She has been widely published in academic journals and speaks frequently for industry organizations such as AIIM, Association of Legal Administrators, Gilbane Conferences, LawNet/ILTA and Cohasset Associates/MER. Galina also serves on the board of ARMA International, a not-for-profit Information Management education organization.

Galina earned her BA from Barnard College and doctoral and master's degrees in Computer Science from Columbia University.

Christopher Fox is a senior principal in CA's Governance Risk and Compliance Manager group. Part of his role is to focus on the evolution of GRC, provide CA thought leadership and to translate new developments into requirements for future versions of our software. Where knowledge has not been fully defined, Chris helps to refine and develop GRC intellectual property, including a risk library, and provide support to CA and the GRC market.

He became interested in GRC through work he performed at the Australian Securities Exchange and furthered his interest working as a director at PricewaterhouseCoopers in banking regulatory projects and in the management of large Sarbanes-Oxley projects. He has also provided IT input into COSO ERM, worked on the Monitor and Evaluate component in COBIT 4.1 and was one of the main authors of ISACA's IT Control Objectives for Sarbanes-Oxley and one of the authors for IT Control Objectives for Basel II. He was a member of the task force that developed OCEG's Red Book on GRC. He is currently working on an ISACA project addressing IT enabled monitoring of controls and a CA project mapping the Uniform Controls Library to FISMA requirements.

Kenneth V. Handal served as executive vice president, office of the chief executive officer, at CA. Until April 2009, he served as executive vice president, global risk & compliance and corporate secretary, with a responsibility for CA's corporate governance, risk and compliance programs, and the internal audit and global security functions. Ken joined the company in July 2004, as executive vice president, general counsel and corporate secretary.

Prior to joining CA, Ken was associate general counsel and served as compliance counsel for Altria, then the parent company of Kraft Foods and Philip Morris. Prior to joining Altria, Ken was a partner with the law firm of Arnold & Porter. Earlier, he was an Assistant United States Attorney for the Southern District of New York, Criminal Division. He also served as a law clerk to Judge Robert A. Ainsworth, Jr. of the U.S. Court of Appeals for the Fifth Circuit.

Ken currently serves on the advisory boards of the Hospital for Special Surgery and Corporate Counsel magazine. He has served on the boards of the National Center for Missing & Exploited Children, The Legal Aid Society, the Association of the Bar of the City of New York Fund, Inc., New York Lawyers for the Public Interest, the International League for Human Rights, the Brooklyn Academy of Music, and the Convent of the Sacred Heart. He also established the in-house Pro Bono Programs at

CA and Altria. Ken is a frequent lecturer at continuing legal education conferences.

Ken earned his law degree from The University of Chicago Law School, where he was managing editor of the Law Review, and his undergraduate degree from Georgetown University.

William E. McCracken is the independent Chairman of the Board at CA. Bill joined CA's Board of Directors in 2005, became Chairman in 2007, and also served as chairman of its special litigation committee.

Prior to joining CA, Bill held numerous executive positions at IBM during his 36-year tenure, most recently as a member of the Chairman's Worldwide Management Council and general manager of IBM's printing division. He previously served as president of IBM's EMEA and Asia PC Company and as the general manager, marketing, sales and distribution for IBM PC Company.

Bill is active in the National Association of Corporate Directors, and is a commissioner of the 2009 Blue Ribbon Commission on Risk Governance. He is also a participant in the Chairmen's Forum of the Millstein Center for Corporate Governance and Performance at the Yale School of Management.

Bill is the president of Executive Consulting Group, LLC, and was a director of IKON Office Solutions. He is board chairman of Lutheran Social Ministries of New Jersey, a member of the New Jersey State Anti-Poverty Network, and a former president of the board of Plainfield Habitat for Humanity.

John Meyer is Vice President of Business Unit Strategy for CA. John has led strategy and product management for multiple business units since he joined CA in 2003. John's broad industry expertise both as an industry analyst and seasoned IT practitioner allows him to infuse CA's strategy with his big picture insights and real world customer driven experience across multiple IT domains.

During his 24 year career in the IT industry he has made significant contributions to the advancement of IT and business alignment. As a senior industry analyst at Forrester Research he provided insight and guidance to many Fortune 500 companies and was a recognized speaker within the IT industry often being quoted by the media. Prior to Forrester Research, John was Director of Enterprise Architecture (EA) for Fortune 50 Fannie Mae. He has also held technology leadership and management positions at other leading companies such as Oracle Corporation, Booz Allen and Hamilton, and Wellspring Resources.

John holds a Bachelor of Science degree in Computer Science from the University of Maryland.

Helge Scheil is CA senior vice president and area manager, responsible for the company's operations in Germany.

Prior to April 2009, Scheil was senior vice president and general manager of the Project and Portfolio Management business unit within the Governance group at CA, responsible for the CA Clarity PPM, New Product Development and Professional Services Automation product lines.

Scheil joined CA with its acquisition of Niku in July 2005. At Niku, he was responsible for all research and development activities and the creation of an innovative, extensible, scalable and fully globalized architecture for Clarity, the market-leading Project and Portfolio Management solution.

Scheil has more than 19 years of experience in enterprise business application development and consulting, a career that took him from Philips Medical System in Germany to Oracle's headquarters in California, where he held various development management positions.

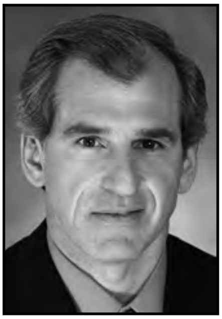
Scheil holds a Bachelor of Science degree in Business and Computer Science from the University of Kiel, Germany.

Alan Srulowitz is vice president of Finance Strategy at CA. In this role, he is responsible for the design and implementation of a Finance Excellence Program to identify and prioritize changes to processes, systems and organizational structure that will improve the efficiency and effectiveness of the Finance organization.

Alan has held various management roles since joining CA in 2004. Prior to assuming his current role he led the Internal Control Function (ICF) to support management's compliance with the Sarbanes Oxley Act. In 2008, Alan was named a "Millstein Rising Star of Corporate Governance" by the Yale School of Management and was nominated for a Corporate Secretary Magazine Award in the "Rising Star" category.

Alan has extensive experience in auditing, finance and operational management. Before joining CA in 2004, Alan was the Controller of the Experience Music Project, an interactive music museum founded by Paul Allen. Earlier, he served in various management roles at Amazon.com supporting the build-out of their Global Logistics Division. Alan began his career as an auditor at KPMG.

Alan earned a Bachelor of Arts degree with high honors at Queens College and a Master of Business Administration degree from Columbia Business School. He is a Certified Public Accountant.



Rob Zanella is vice president of IT Compliance for CA and is responsible for all compliance activities within Information Technology. Rob joined CA in 2005 as director of Internal Audit to develop the company's first IT Audit practice. Upon establishing the practice, Rob next assumed responsibility for the IT Compliance function to advise on controls optimization opportunities and to manage CA's IT risk and controls profile.

Rob has 25 years of IT experience in operations, software development, project management, and auditing. Before joining CA, he was director of IT Audit for 5 years at SIAC, the technology arm of the NYSE. Prior to the NYSE, Rob was a senior manager at Deloitte & Touche for 7 years, implementing ERP solutions as part of their Enterprise Risk Services group for several large clients. In addition, he held various software development and project management positions within Savings Bank Trust Company and Union Savings Bank while developing and implementing lending software.

Rob has been a Certified Information Systems Auditor (CISA) as certified by ISACA (Information Systems Audit and Control Association) since 1995. He holds a Bachelor of Science in Computer Science from Hofstra University and a Master of Business Administration from Adelphi University.

Contributors

Christopher Boswell

Margaret Brooks

Terrence Clark

David Hurwitz

Lynne Iati

Lily Kang

Elizabeth Kelly

Tom Kendra

Yves Le Roux

Lynne Mahoney

Bill Manago, CRM

Michael Mattia

Thomas McHale

Jeffrey Meyer

Jose Mora

Kristen Perdue

Steve Romero

Michael Sanchez, Sirius Solutions

Peter Stapleton

Kurt Steinle

Robert Stubbs

Andrew Wittman

Acknowledgments

The authors gratefully acknowledge the help and support of a number of individuals who made up the project team.

Their CA colleagues: Lynne Mahoney, whose determination, resourcefulness and editing drove the book to completion; Sumner Blount, who both authored his own chapters and made invaluable contributions to many others; Connie Smallwood and Karen Sleeth, who worked tirelessly to establish the CA Press infrastructure; Andrew Wittman, whose critical thinking helped both launch and complete the project; Margaret Brooks for contributing her subject matter expertise to the reviewing effort; Lily Kang for her valuable work on "Governance of Risk and Compliance"; Michael Mattia for his widespread contributions to "IT Governance, Risk and Compliance"; Elizabeth Kelly for her substantial work on "Governance and Portfolio Management" and Steve Romero for reviewing same and contributing blog posting; Robert Stubbs for his extensive editing of "The Regulatory Environment"; Bill Manago, CRM, for lending his expertise to "Information Governance"; Jeffrey Meyer for his extensive work on "Governance and Sustainability". Terrence Clark for reviewing same and contributing his blog posting.

Their partners at Apress, Inc.: Jeffrey Pepper and James Markham (the editorial team); Tiffany Taylor for her editing work; Tom Welsh for fact checking; Frank McGuckin for directing the production of the book; Anna Ishchenko for her work on the cover; April Milne and Jerry Votta for the art; and especially James Keogh for all of his work on the book.

Introduction

Business and public sector leaders today face an unprecedented challenge of compliance and risk management.

A long-standing trend toward increased regulation became a flood with the economic crisis of 2008. Combined with the clamor for improved enterprise risk management and the growing complexity of multi-national compliance, these conditions present executives with a dramatically new and confusing array of questions and challenges.

Governance should offer solutions, but it is increasingly clear that yesterday's governance practices aren't up to the task. In both design and implementation, they are too disconnected and incomplete to fully address our complex compliance and risk management puzzle. Executives get only fragmented views of their true business performance, and inefficiencies drive up costs.

We at CA can look at this challenge with a unique perspective. As Computer Associates, our company directly experienced the consequences of inadequate governance, including an investigation in 2002 that resulted in an agreement with the government to improve accounting and other business processes. Those who know this history may wonder why CA is qualified to advise on governance at all. My answer is, who could better understand the issues and the consequences of inadequate governance than CA?

In our exhaustive efforts to successfully rebuild our company, we have worked with the leading thinkers in governance and ethics. Where some companies view governance as a "nice to have", seeking out and implementing best practices in the field was essential to CA's future. That imperative allowed us to devote a significant amount of energy and resources to the task, and attracted some of the best people in the field to CA. Our improvements enabled us to fulfill our obligation to the government, stabilized the company, and propelled us into a new era of growth with an unusually strong foundation of leading governance practices.

In this book, we have captured that expertise for the benefit of other organizations. Each chapter is authored by a CA executive with in-the-trenches responsibility for vital governance processes, and in some cases the development of governance solutions. Those solution experts have worked with thousands of clients, giving them unparalleled insight into the most practical and productive governance practices.

Our collaboration as a team, leveraging both CA and external experience, led us to formulate a new approach to governance that unifies compliance and risk management to increase the effectiveness, and decrease the cost, of both. The core of this unified approach is the centralization of policies across organizational silos. Polices include any requirement on the IT infrastructure, employee behavior, or business processes that enable an organization to reach its goals. Too often these policies are recorded, implemented and measured in organizational silos. But for really effective governance, we need to break down the walls between those silos and devise common approaches to managing policies, measuring performance against them, and ensuring compliance with them.

And, this management of policies must be executed with formality, rigor and transparency. That allows governance to become part of the fabric of an organization with defined, documented, communicated and repeatable processes. With this approach, we can develop and maintain policies that address the current governance need—and have enough flexibility to address evolving market conditions.

This unified governance approach also offers a broad view of risk across the enterprise. It standardizes risk management rather than isolating it to individual regulatory or operational silos. Organizations gain not only greater insight into risk within business units, but also can evaluate the interactions of risks across the enterprise and more easily identify emerging risks before they become critical to the entire organization.

And finally, risk management and compliance will be under control.

Jacob Lamm
Executive Vice President, CA, Inc.

CHAPTER

1

The Rise of Governance

by Jacob Lamm

Rumblings deep in the world economy drew little attention in 2006. Interest rates rose modestly and housing prices stopped their steep ascent in the United States, signaling an economic swing that financial institutions normally handle in stride.

However, this time conditions were different. Proven techniques for dealing with economic swings couldn't handle the events that were to unfold at lightning speed. The United States housing bubble finally burst in 2008—creating the most serious financial crisis since the Great Depression.

The house of cards tumbled, taking with it several cornerstone financial institutions. Certain corporate leaders were stunned and wondered how such strong organizations with sophisticated technology at their fingertips failed to foresee and react to such a devastating exposure to risk. And many were surprised at how large the impact was. Banks and other financial companies, as well as their investors, were dramatically hit as the effect rippled throughout the world.

The reason was, in essence, tunnel vision. Leaders of some of the world's marquee corporations were blindsided because their internal corporate monitors were unable to piece together regulatory, operational, and risk-management indicators that pointed to irregularities and which collectively jeopardized the underpinnings of their businesses.

The subprime-mortgage crisis was the latest event to highlight shortcomings in corporate governance. Many past failures, including that of Enron, were often the result of poor corporate oversight. In some cases, out-and-out fraud was involved. However, fraud that goes undetected or unaddressed is, to some extent, a failure of corporate governance.

As these cases appear in the news, cries for stronger and more effective governance, often accompanied by more stringent governmental regulation, go out. In many cases, these governance "holes" are plugged or at least mitigated—until the next governance crisis. This creates a need for increased emphasis on improved governance, and the cycle continues.

What Does Governance Really Mean?

Like many terms in the public eye in recent months, *governance* is in the eye of the beholder, and definitions can vary from one author to another. But the essence of the definitions is generally the same. *Governance* is the leadership, organizational structures and processes that help ensure that an organization's functions sustain and extend its strategies and objectives. Put more simply, it is the culture, policies, procedures and controls that help ensure a company will meet its business goals.

Governance is "everybody's job." However, the key governance responsibilities are typically entrusted to the Board of Directors and the executive management of a corporation who are responsible for providing the oversight that is intended to help ensure that a company meets its goals.

When considering the broad topic of governance, an obvious question might be "Governance of *what*?" The answer is "Governance of everything that relates to the operation of the company." This includes a wide variety of areas, such as finance, marketing, product development, security, information technology (IT), human resources, compliance, risk, and others.

There are a few generally accepted terms for the different areas of governance. Let's review the most common ones:

Corporate governance focuses on the effectiveness of the corporation as a whole, including meeting defined risk and compliance goals, so as to meet the overall business objectives. This is the responsibility of executive management, the Board of Directors, and often the legal department.

Corporate governance is the application of formality, rigor, and transparency to a unified framework of corporate policy, to help ensure that an organization takes on only prudent risks in its quest to return stockholder value and succeed in the market. (See the section "A New, Unified Approach" later in this chapter for more on formality, rigor, and transparency.) Risks that affect the achievement of strategic goals must be understood, properly assessed, and managed effectively.

Operational governance focuses on the planning and execution of projects and resources associated with key business operations, such as IT and product development. The focus here is on ensuring that the operational processes of the company are effective and efficient, and that assets of all types are used effectively to help meet corporate goals.

Governance, risk, and compliance (GRC) focuses on the activities related to the governance of regulatory requirements, enterprise risk areas such as financial and IT risk, compliance controls, and information across the enterprise. GRC is not a specific function in an organization, but rather an integrated approach across multiple business functions related to the management of risk, controls, and compliance.

Historically, this management has often been handled by disparate groups with minimal interaction. More recently, there's been a trend toward a more unified view of these areas to help controls costs, eliminate redundancy, and improve the quality of the information that is used to make decisions related to risk and compliance.

GRC includes several different but related areas:

- *Enterprise risk management* focuses on predicting and managing events that might impact the achievement of business goals.

- *Financial GRC* relates to the quality, timeliness, and transparency of financial statements and transactions of the company.

- *IT GRC* relates to managing IT risk and ensuring that the IT infrastructure supports corporate compliance needs.
- Finally, *information governance* focuses on ensuring that the company's information assets are known, categorized, and available when needed.

Figure 1-1 illustrates the relationships of these areas to each other.

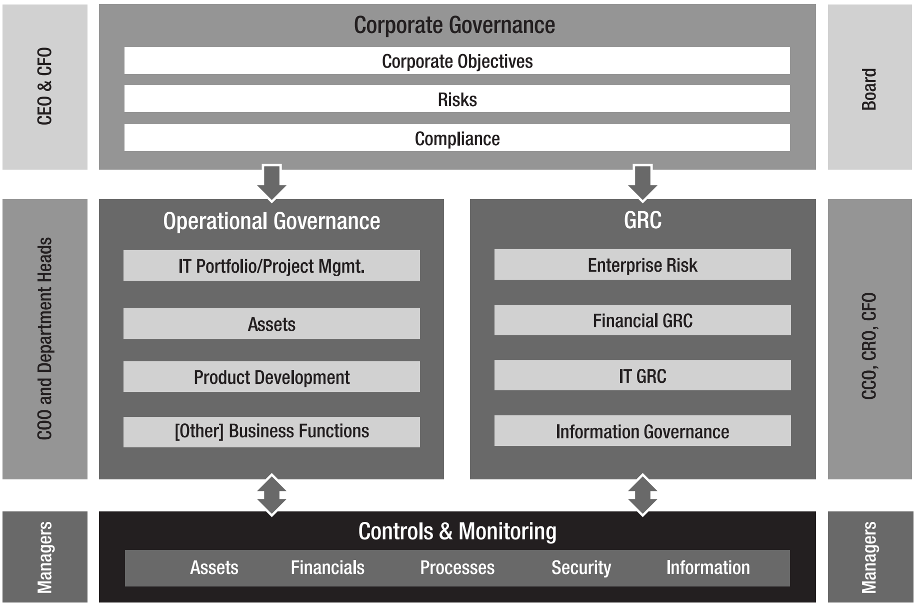


Figure 1-1. Areas of governance

A key element of all these different areas of governance is the design, implementation, continuous monitoring, and auditing of compliance controls to assess the organization's vital signs, enabling corporate leaders to oversee activities and intervene, if necessary, to put the organization back on course.

The Drivers for Governance

Governance is far from a new concept; corporations have long practiced it. But there *has* been a change in the level of attention given to governance. This increased emphasis has been driven by the needs of the corporation, the stockholders, and regulatory bodies. The following are some of the key business drivers for improved corporate governance.

The Rise of Risk

Recent economic events have shown clearly that the improper assessment and management of risk can have a catastrophic impact on a corporation. The precise causes of the recent economic crisis are open to debate, but it's clear that ineffective or nonexistent risk management was a significant contributing factor.

In its policy paper "Climbing Out of the Credit Crunch",[1] the Association of Chartered Certified Accountants, the international accountancy body, pointed to the failure of corporate governance at some financial institutions as the underlying cause of this catastrophe. This failure led to excessive risk-taking and insufficient risk management.

Where did this emphasis on risk come from? From a painful history.

On July 30, 2002, the Sarbanes-Oxley Act (SOX), which implemented some of the most far-reaching reforms of public companies since Franklin D. Roosevelt's New Deal, was signed into law. SOX sought to increase transparency, improve the accuracy of financial statements, and reduce potential conflicts of interest.

Prior to SOX, outside auditors could enter into lucrative consulting contracts with clients they audited. Securities analysts could issue "buy" recommendations for corporations who paid substantial bank service fees to the investment banking side of the house. The extensive use of stock options to compensate executives at certain corporations created pressure

[1] Association of Chartered Certified Accountants, "Climbing Out of the Credit Crunch," September 2008, http://www.accaglobal.com/allnews/national/australia/3150218 (accessed 1 December 2009).