SAP® GRC FOR DUMMIES®

by Denise Vu Broady and Holly A. Roland

WILEY
Wiley Publishing, Inc.

SAP® GRC FOR DUMMIES®

by Denise Vu Broady and Holly A. Roland

WILEY
Wiley Publishing, Inc.

SAP® GRC For Dummies®

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

For technical support, please visit www.wiley.com/techsupport.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Control Number:

ISBN: 978-0-470-33317-4

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

WILEY

About the Authors

Denise Vu Broady: Denise is SAP's VP of Strategic Applications. She runs the SAP CFO Center of Excellence, a cross-solution team responsible for enabling customers to use SAP technology and products to transform the Office of the CFO. She has business development responsibility for the entire CFO portfolio of solutions, including Governance, Risk & Compliance (GRC); Enterprise Performance Management (EPM); and Spend Optimization. Denise has over 11 years of SAP-related experience. At SAP she has specialized in bringing new products to market; Denise played a central role in the launch of xApps, NetWeaver, Payroll Change Management, GRC and EPM. She came to SAP via the acquisition of TopTier where she was Product Manager. Earlier in her career, Denise gained hands-on SAP experience as a consultant on multiple R/2 and R/3 technical and functional projects. Denise has a BS in Management Science and Marketing from Virginia Tech and resides in New York City.

Holly A. Roland: Holly is the vice president of marketing for SAP's Governance, Risk and Compliance (GRC) business unit. In this role, she is responsible for product strategy and marketing for SAP's GRC products. Holly created the industry-leading executive advisory board for GRC, composed of customers, partners, and SAP executives, which facilitates collaboration among business executives and industry leaders to identify common GRC challenges, develop GRC best practices, and conceive of supporting technology solutions. Holly was instrumental in the integration of Virsa Systems and the successful design and execution of SAP's GRC product launch in 2006. She publishes articles and serves as an expert speaker for international events and forums on GRC topics. Holly has more than 15 years of experience in financial accounting and reporting, regulatory compliance, business analytics, and enterprise software marketing and development. Prior to joining SAP, she led product strategy, marketing, and product management operations at Virsa Systems, Oracle Corporation, Hyperion Solutions, and Movaris. Holly also served as a public accountant for PriceWaterhouseCoopers where she audited large public companies and provided business consulting. Holly graduated cum laude from Santa Clara University with a BS in Commerce. She is based in SAP Labs in Palo Alto, California.

Dedication

To my husband for always listening, no matter how long my stories take. And to Safra, my guiding light. —Holly

To Tsafi, my better half, who has been extremely patient and supportive with a hectic year of travel and work and letting many chapters of this book join us on vacations and weekends. —Denise

Authors' Acknowledgments

This book would not be possible without the help and support of many, many people. Our colleagues at SAP were very generous with their time and research materials, providing us with interviews, research materials, and even whole sections revised or written in their hand.

Special thanks are due to Gary Dickhart, who couldn't stop writing (we're waiting for your GRC book, Gary), David Milam and Dave Anderson, who helped us greatly improve our chapter on risk management (Chapter 2). Mark Crofton made important contributions to the financial compliance chapters in Part II. Marina Simonians and David Ahrens provided tremendous support for Part III, "Going Green." Paul Pessutti helped us with interviews, reviews, and revisions in the very complex area of global trade (Chapter 8), as well as our related Part of Ten (Chapter 17). Christian Berg, who is both a colleague and an expert in the area of sustainability, shaped Chapter 14. We would also like to thank Karan Dhillon for his excellent interview and research materials; his input can be seen throughout the book, as can the influence of Bob Crochetiere, whose interview was also formative. We also extend our appreciation to the following people who helped us in bringing this book together: Nenshad Bardoliwalla, Wolfgang Bock, Ben Cesar, Lee Dittmar, Ravi Gill, Marko Langes, Melissa Lea, Joe Miles, Phil Morin, Jim Mullen, Tom Neacy, Barry Nemmers, Eric Solberg, Axel Streichardt, and Greg Wynne. Thank you for the time you spent working with us, despite very hectic schedules.

We'd like to thank the writers at Evolved Media: Dan Woods, Deb Cameron, Charlotte Otter, D. Foy O'Brien, James Buchanan, Kermit Pattison, David Penick, and Justin Jouvenal.

We would also like to extend our sincere thanks to the great people at Wiley, especially Katie Feltman, Beth Taylor, and Linda Morris, for all their hard work, dedication, and perceptive editing.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at `www.dummies.com/register/`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Beth Taylor

Development Editor: Linda Morris

Senior Acquisitions Editor: Katie Feltman

Copy Editor: Beth Taylor

Editorial Manager: Jodi Jensen

Editorial Assistant: Amanda Foxworth

Sr. Editorial Assistant: Cherie Case

Cartoons: Rich Tennant (`www.the5thwave.com`)

Composition Services

Project Coordinator: Patrick Redmond

Layout and Graphics: Stacie Brooks, Alissa D. Ellet, Reuben W. Davis, Christine Williams

Proofreader: Evelyn W. Still

Indexer: Potomac Indexing, LLC

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Acquisitions Director

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Joyce Pepple, Acquisitions Director

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Contents at a Glance

Table of Contents

Introduction

GRC is an acronym that may be Greek to the uninitiated, but chances are if you picked up this book, you are at least interested in knowing what it means. And even if not everyone knows what GRC means, the concepts involved are ones that everyone understands.

The G is governance. In short, this means taking care of business, making sure that things are done according to your standards (and those of the ever-present regulators, not to mention your company's Board of Directors). It also means setting forth clearly your expectations of what should be done so that everyone is on the same page with regard to how your company is run.

The R is risk. Everything we do involves an element of risk. When it comes to running across freeways or playing with matches, it's pretty clear that certain risks are just not to be taken. When it comes to business, however, risk becomes a way to help you both protect value (what you have) and create value (by strategically expanding your business or adding new products and services).

The C is what everyone knows about — compliance with the many laws and directives affecting businesses (and citizens) today. One of the authors of this book would also like to extend that C to controls, meaning that you put certain controls in place to ensure that compliance is happening. This might mean monitoring your factory's emissions or ensuring that your import and export papers are in order. Or it might just simply mean that the same person is not creating vendors and cutting checks to her brother-in-law Frank on the sly. The C relates to laws as familiar as Sarbanes-Oxley (SOX) or as emergent as Europe's REACH (if we've got you on that one, see Chapter 12).

But when you put it all together, GRC turns out to be not just what you have to do to take care of business, but a paradigm to help you grow your business in the best possible way and — even more — to figure out what that way is.

About This Book

When we decided to write a book about GRC, we thought about writing a book for experts, a thought-leadership book. And although this book is no slouch in the area of thought-leadership (if we do say so ourselves), we decided that what was needed the most was a way to start the conversation about GRC. What are you doing, in terms of governance, risk, and compliance? What should you be doing? And do you know that it's a much bigger picture than you realize, encompassing areas like sustainability and dovetailing very nicely with developing and executing your key business strategies?

That's why this book was originally going to be called *GRC For Dummies*. But (as you can see by the title), it's *SAP GRC For Dummies*. That's a bit of a misnomer because unlike classics like *SAP NetWeaver for Dummies*, this book is not all about SAP software. It's mainly about GRC. But SAP has leading software for GRC, so at the end of relevant chapters, we tell you about products like SAP GRC Risk Management and how it can help you. This book could have been all about SAP GRC, easily — there are probably areas that SAP covers that you don't even know about. (For example, we bet you didn't know that SAP is a leader in the area of software for environmental management.) But just a disclaimer before we start—there's a lot more to learn about SAP GRC than we cover in this book. We focus on giving you the background to get started conceptually in the most important areas.

Now that we've explained a bit about the book, are you ready to get started and to become well-versed in GRC? That way, if you need a conversation stopper for Aunt Ida at Thanksgiving — or, better, a conversation starter when talking to almost anyone about what it takes to succeed in business today — you'll be prepared.

Foolish Assumptions

In writing this book, we made a few assumptions. If you fit one of these assumptions, this book is for you:

- You're interested in GRC from a corporate perspective. You can think about GRC from an individual perspective (paying your taxes, protecting your identity, and balancing your checkbook, for example), but this book talks about how to use GRC to improve your company, not your household.
- You have some background in common business terms like profit and loss and common accounting terms such as general ledger and purchase order.
- You're not adverse to acronyms. GRC can be a little like alphabet soup at times. For clarity, we provide a glossary to help you find your way through the more obscure TLAs (three-letter acronyms).

How This Book Is Organized

To help you get a better picture of what this book has to offer, we explain a little about how we organized it and what you can expect to find in each part.

Part I: Governance, Risk, and Compliance Demystified

You need to have a good foundation in place to see how GRC can help you. Part I starts out with the ABCs of GRC to give you the big picture and then heads straight into risk and governance to round out your education.

Part II: Diving into GRC

The C in GRC is for compliance, and Part II takes you through some of the regulations companies must comply with and the corporate scandals that led to those regulations. Once you know about them, what do you do about them? This part also addresses tools like access control and process control that can help you ensure compliance. And, since globalization has brought so many companies into the global trade arena, Part II provides details about the compliance-related issues you need to know about to effectively source goods from or sell goods to other countries.

Part III: Going Green

Saving the planet is on everyone's minds these days, and it's not just good policy—it's good business, too. Part III addresses how you can ensure that your company's policies about people, processes, and products keep you compliant with the law and enable you to deepen your company's shade of green.

Part IV: Managing the Flow of Information

GRC is strategic. It can provide you with new insights into how to run your business. Part IV first delves into the flow of information in the enterprise from an IT GRC perspective, ensuring that data is kept secure and private, for example. It then turns to the important area of sustainability reporting, the nonfinancial reporting that more and more companies are doing and which is so important to a variety of stakeholders, from employees to investors to nongovernment organizations such as Greenpeace. Finally, and perhaps most importantly, Part IV addresses how you can use what you learn about your company through a program of integrated GRC to help you envision and execute the best possible corporate strategy.

Part V: The Part of Tens

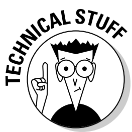
Maybe the Part of Tens are your favorite part in any *For Dummies* book (we always look for them). Here you'll find best practices for GRC implementation and best practices for global trade. You'll also find pointers to resources to help you in your quest to become an expert in the area of GRC, from books to blogs to web sites.

Glossary

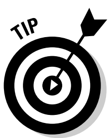
As you read this book (or skip from chapter to chapter, section to section, looking over only those parts that interest you), you may have additional questions in some areas. That's why we include a comprehensive glossary, chock full of definitions of the many terms that you're likely to encounter as you learn more about GRC.

Icons Used in This Book

To help you get the most out of this book, we use icons that tell you at a glance if a section or paragraph has important information of a particular kind.



This icon indicates information that is more technical in nature, and not strictly necessary for you to read. If technical jargon gives you a headache, feel free to skip these.



When you see this icon, you know we're offering advice or shortcuts to quickly improve your understanding of GRC concepts.

Look out! This is something tricky or unusual to watch for.

This icon marks important GRC stuff you should file away in your brain, so don't forget it.

Where to Go from Here

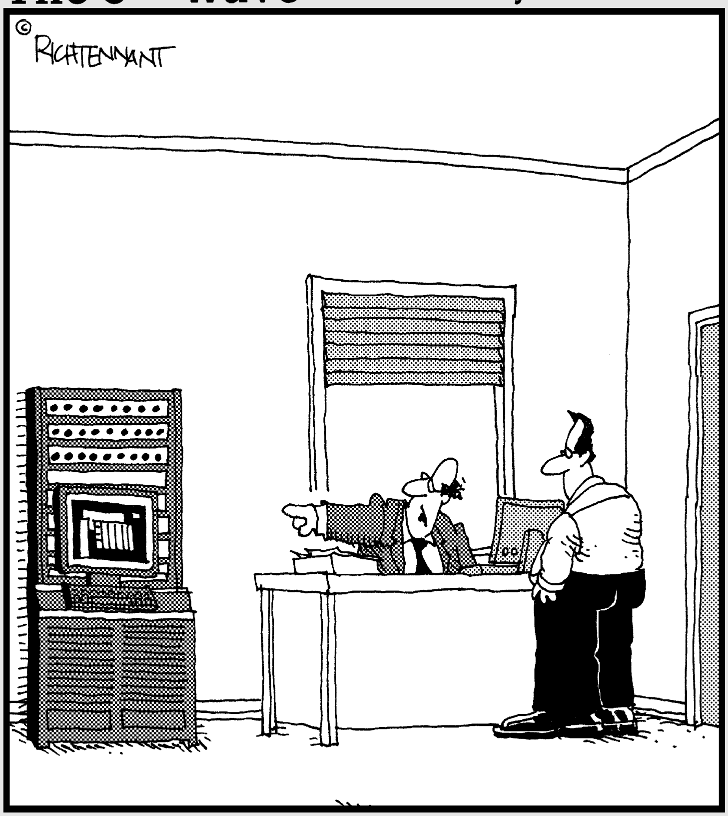
If you're new to SAP GRC or GRC in general, your next step is to head straight to Chapter 1, which gives you the ABCs of GRC, as well as providing food for thought about what GRC can do for you.

If you're a professional in a particular area — such as global trade, risk management, or IT governance — you could decide to visit particular chapters in no particular order. But (and we're probably biased) we think the best way forward from here is straight into Chapter 1 (with a few intervening pages to entertain you on your way there).

Part I

Governance, Risk, and Compliance Demystified

The 5th Wave By Rich Tennant



"We've got a machine over there that monitors our quality control. If it's not working, just give it a couple of kicks."

In this part . . .

You start your GRC education with the ABCs of GRC. Even if you're a GRC expert, Chapter 1 gives you the panoramic view of how GRC can help you run your business better. You then move into the all-important area of risk — nothing ventured, nothing gained. You find out that properly managing risk is one of the most important factors for business success today. And to put those management strategies into practice systematically, Chapter 3 lays a solid governance foundation, uncovering what governance means and all its implications.

Chapter 1

The ABCs of GRC

In This Chapter

- Getting to know GRC
- Discovering the GRC stakeholders
- Understanding GRC by the letters
- Deciding on your approach to GRC

Governance, Risk, and Compliance, almost always referred to as GRC, is the latest addition to the parade of three-letter acronyms that are used to describe the processes and software that run the business world. The goal of GRC is to help a company efficiently put policies and controls in place to address all its compliance obligations while at the same time gathering information that helps proactively run the business. Done properly, GRC creates a central nervous system that helps you manage your business more effectively. You also derive a competitive advantage from understanding risks and choosing opportunities wisely. In other words, GRC helps you make sure that you do things the right way: It keeps track of what you are doing and raises an alert when things start to go off track or when risks appear.

This opening chapter takes you on a top-to-bottom tour of GRC to help you understand in greater detail what GRC means and what companies are doing to lower the costs and create new value.

Getting to Know GRC

GRC is not just about complying with requirements for one quarter or one year. Rather, those who are serious about GRC, meaning just about everyone these days, seek to create a system and culture so that compliance with external regulations, enforcement of internal policies, and risk management are automated as much as possible and can evolve in an orderly fashion as business and compliance needs change. That's why some would say that the C in GRC should stand for controls: controls that help make the process of compliance orderly and make process monitoring — and improvement — easier.

Some parts of the domain of GRC — measures to prevent financial fraud, for example — are as old as business itself. Making sure that money isn't leaking out of a company and ensuring that financial reports are accurate have always been key goals in most businesses—only recently have they attained new urgency.

Other parts of GRC related to trade compliance, risk management, and environmental, health, and safety regulations are somewhat newer activities that have become more important because of globalization, security concerns, and increased need to find and mitigate risks. For example, to ship goods overseas, you must know that the recipient is not on a list of prohibited companies. These lists change daily. Growing concern about global warming and other pressures to reduce environmental impact and use energy efficiently have increased regulations that demand reporting, tracking, and other forms of sociopolitical compliance. Companies are also interested in sustainability reporting, measuring areas such as diversity in the workplace, the number of employees who volunteer, and environmental efforts, so that companies can provide data about corporate social responsibility. Financial markets punish companies that report unexpected bad news due to poor risk management.

One simple goal of GRC is to keep the CFO out of jail, but that description is too narrow to capture all of the activity that falls under the umbrella of GRC. (It's also an exaggeration; the truth is that simple noncompliance is more likely to result in big fines rather than a long trip to the big house. But, that said, most executives prefer to leave no stone unturned rather than risk breaking rocks in the hot sun.) Most companies now face demands from regulators, shareholders, and other stakeholders. Financial regulations like Sarbanes-Oxley (SOX) in the United States and similar laws around the world mean that senior executives could face criminal penalties if financial reports have material errors. (For more on Sarbanes-Oxley, flip ahead to Chapter 4.) All of this means a lot more testing and checking, which is costly without some form of automation.

REMEMBER

If GRC seems like a sideshow to your main business, remember you can't get out of it, so you might as well make it work for you, not against you. At first, especially in 2004 — the first year in which Sarbanes-Oxley compliance became mandatory — companies frequently engaged in a mad rush, throwing people, auditors, spreadsheets, and whatever resources were required at the problem. Although the rush to comply was heroic, it was far from efficient. Now companies are understanding how to turn GRC activities into an advantage.

The question every company must answer is the following: Will we do the bare minimum to make sure that we stay out of trouble, or can GRC become an opportunity for us to find new ways of running our business better?

Because it is concerned with creating a sustained stream of high-quality information about a business, GRC has a large overlap with Corporate Performance Management (CPM), a topic we cover in greater detail in Chapter 15.

If the burdens of GRC are a cloud, the silver lining is that in learning how to keep track of business in greater depth, GRC activities are transformed from an annoyance to a gateway to an expanded consciousness in a company, which can lead to better performance, reduced costs, and competitive advantage. GRC is part of the natural process of turning strategy into action, monitoring performance, and tracking and managing the risks involved. Choosing to see GRC as an opportunity can mean significant savings in auditing costs, creating new sources of information for improving processes, finding risks earlier, and most of all, avoiding those nasty surprises that spark a punishing reaction in the stock market.

Getting in the Business Drivers' Seat

In some ways, GRC is nothing new: Almost every activity under the bailiwick of GRC has been going on for quite some time in the business world. The segregation of duties that is required by Section 404 of Sarbanes-Oxley has always been part of an auditor's toolkit of recommendations when it comes to preventing fraud. Companies have always been under the obligation to report financial results accurately, to comply and report on their performance with respect to environmental, safety, and trade laws, and to identify risks as early as possible. Every well-run company — whether private or public — puts its own unique self-inflicted policies in place and makes sure that they are being followed. As times change, all of these measures must be updated.

What caused the birth of GRC as an area of focus for companies and those who provide consulting services and software was a perfect storm of urgency about various issues. Consider the following elements of that perfect storm:

- In the wake of the go-go culture of the Internet investing boom of the late 1990s, massive, systematic fraud was revealed at major companies such as Enron, WorldCom, Adelphi, and others. In many cases, the controls and external forms of scrutiny that were in place to stop such bad behavior had failed for many different reasons, including fraud, conflicts of interest, and other forms of malfeasance.
- At the same time, the terrorist attacks on September 11, 2001 led to a worldwide tightening of controls on trade, especially with respect to sales of certain types of products or materials that were deemed dangerous if fallen into the wrong hands. For example, ITT shipped night vision goggle components to China and other countries, resulting in a U.S. Department of Justice fine of $100 million.

- The third force driving the urgency of GRC is the rising concern about energy consumption and the environment. Instability in the Mideast, scarcity of oil supply due to increased consumption, and lack of new oil discoveries have driven oil prices to record highs. Worries about global warming have caused a new wave of demands for energy efficiency, reductions in environmental impact, and a desire for companies to demonstrate the long-term sustainability of their operations.

Lawmakers around the world awoke to this crisis and felt a burning need to DO SOMETHING! A debate still rages about the wisdom of the governmental response, but there is no mistaking the result: an across-the-board increase of the volume and urgency of compliance activities. But seeing GRC only in terms of Sarbanes-Oxley and financial compliance is a mistake. Although complying with Sarbanes-Oxley and other similar laws that have been enacted worldwide certainly spurred many companies to action, after they got started, companies realized that there was a whole other field of compliance, risk, and governance-related activities that needed to be performed with greater attention and efficiency.

Investors, along with governments and regulators, insurance companies, ratings agencies, and activist stakeholders have also joined in increasing the urgency with respect to transparency and accuracy of information about the company's operations and actions taken to mitigate risks and issues. Stock markets have dealt brutal punishment to companies that report problems with internal controls or other negative surprises. Consider these statistics:

- According to a McKinsey Study, investors in North America and Western Europe will pay a premium of 14 percent for companies with good governance, as shown in Figure 1-1.
- The difference in stock market value for companies that had good internal controls versus those that did not is 33 percent.
- AMR Research predicted that companies would spend $29.9 billion on compliance initiatives in 2007 alone, up 8.5 percent from the previous year, indicating that GRC spending continues to grow as companies cope with the myriad challenges in this area.

All of these forces combined led to the creation of the domain of GRC as companies realized that an ad hoc approach to meeting these demands was too expensive and actually increased risk for the companies because they couldn't mitigate issues they didn't know about.

The difficulty facing most companies right now is not how to meet these GRC challenges — the fact is, the forces that are driving increased attention to GRC are not optional for the most part and companies have no choice but to comply — but rather *how* to comply efficiently in a way that produces benefits. GRC shouldn't be just a cost that does nothing else for your business, but that may become your attitude if you want to be just good enough to barely meet minimum compliance standards.

**Investors Reward Good Governance…
and Penalize Poor Governance**

Investors worldwide will pay a premium of 14% or more for shares in companies with good governance.

McKinsey & Co. Global Investor Survey

But companies with internal controls deficiencies experienced significant declines in their market caps:

2004 Disclosure Examples: Company/Market Value	Disclosure	% / Mkt Cap Decline
Adecco SA $12.6 billion Jan. 12	Company delays financial statements. Internal control deficiencies	-38% $4.9 billion
Goodyear Tire & Rubber $1.7 billion Feb. 11	Company has not yet completed the implementation of its plan to improve internal controls	-18% $320m
MCI $5.4 billion Apr. 29	Material weaknesses – lack of systematci and reliable internal controls	-17% $935m
INVESTORS FINANCIAL $2.9 billion Oct. 21	Material weakness discovered during review of internal controls	-16% $475m
FLOWSERVE $1.3 billion Oct. 27	Material weakness in internal controls; two quarterlies overdue	-11% $152m

Figure 1-1: Rewards for good governance.

One way of thinking of GRC is to compare the process of managing a company to driving a car. When you drive a car, you have a certain set of rules that you are expected to abide by. You have to have a driver's license and insurance. Your car must be inspected for compliance with safety and environmental laws. When you are driving, you are encouraged by law enforcement and penalties to drive within speed limits and other restrictions. You may have your own rules about driving, such as never driving while talking on your cell phone in order to be as safe as possible. Other activities such as maintaining the car are up to you and various drivers will have different approaches. Some will change the oil more often than recommended or rotate tires frequently, some will use premium gas, and so on.

What has happened with GRC, to use the driving analogy again, is that the laws for everything related to driving got tighter and more restrictive and the penalties got higher. In addition, the rewards for driving efficiently and safely became much higher. So, you can now figure out how to drive just to keep out of trouble with external watchdogs, or you can figure out how to drive in a new more efficient way that better helps your business win in the marketplace, while still playing by all the rules.

GRC is a new management mentality. The bad news is that more work is required to comply with regulations. More testing and controls have to be in place and the organization has to be carefully designed. As exceptions to policies occur, behavior must be checked and monitored. As people are promoted or job descriptions change, controls must be put in place so that compliance can be maintained. New forms of data must be captured and consulted. Risks must be proactively discovered while they are still small enough to manage. Without a doubt, this brave new world requires more work, and there is a shortage of trained people and expertise to carry it out.

The upside of GRC is that in addressing these issues systematically, the culture and performance of a company improves. In many ways, GRC is concerned with meta processes, which are those that look at the shape and flow of information in other processes in order to identify weak points. Controls and compliance are only one result of GRC: They put the C in GRC, if you will. When properly addressed, GRC helps identify ways that core business processes can be improved. Identification of risks also leads to discovery of opportunities. Governance processes can help create orderly ways to evolve a company, and improve program and change management across the board.

Getting Motivated to Make the Most of GRC

Although concern about GRC is growing, most companies that have engaged in a program of GRC are usually reacting to some pressure or concern that takes GRC from a necessary evil to an initiative that can really benefit the company if is executed thoroughly and efficiently. A serious approach to GRC may flow from any or all of these motivating forces that we discuss in the following sections.

Complying with financial regulations

New laws in the United States and in many other countries mean that if serious errors in financial reports are found, those responsible will face criminal prosecution. Section 302 of Sarbanes-Oxley says exactly this, and prosecutors around the nation have shown great eagerness to enforce this law.

It is not just American companies that are facing such dramatic penalties. See the “A global reaction to improve governance” sidebar later in this chapter for more on changes to GRC laws in other countries around the world. Governments of most of the largest economies have passed their own forms of legislation increasing the level of scrutiny about financial reporting and controls.

The driving force behind this regulation is the fear that inaccurate financial reporting will damage the financial system. Without accurate financial information, investors will have little to go on when making decisions about where

The march of the three-letter acronyms

The world of enterprise software has given birth to many Three-Letter Acronyms, called appropriately by yet another three-letter acronym: TLA. Here is a sample of the most common TLAs:

- Enterprise Resource Planning (ERP) software emerged in the 1990s to provide a complete financial model of a business along with tracking many other aspects. ERP was about closing the books faster and tracking the key financial and management processes of a business.
- Customer Relationship Management (CRM) software emerged in the late 1990s to give a name to software that tracked sales, service, billing, and other activities related to customer interactions with a business. CRM was about getting closer to the customer.
- Supply Chain Management (SCM) software emerged in the 1990s to track the flow of goods and manufacturing processes among a distributed network of partners working together. SCM helped manage increased specialization, outsourcing, and globalization.
- Product Lifecycle Management (PLM) software emerged in the 1990s to give a name to the processes related to creating new products, bringing them to market, and improving them. PLM was about helping increase the speed of product development.
- Governance, Risk, and Compliance (GRC) software emerged in the 2000s to automate controls to facilitate compliance with financial, environmental, health, and safety, and trade regulations, enforce internal controls, increase the efficiency of audits, identify risks, and employ proper governance procedures to keep all of these activities up to date and effective.

to place their money. If confidence drops too far, all companies, not just those who have engaged in bad behavior, will find it harder and more expensive to raise money. This is not the first time that such fears have been raised and reporting requirements have been tightened. Even the powerful tycoons of the Robber Baron era had bankers insisting on better accounting.

So, while compliance with regulations aimed at improving financial reporting and governance is really just one piece of the puzzle when it comes to GRC, fears related to such compliance are clearly the force that has driven most companies to action.

Failing an audit

There is nothing like failing an audit to spur companies to improve their GRC processes. In the wake of a failed audit, which must be reported in public financial statements, investors frequently lose confidence and sell stock.

Nowadays, audits can fail for more reasons than ever. Discovery of fraud or other bad behavior is of course the most dramatic reason. But in the face of tighter regulations for governance and reporting, audit problems can include the lack of adequate controls, improper segregation of duties, insufficient oversight of the creation of financial reports, and many other causes. So even if nothing is wrong, you can fail your audit for not having sufficient documentation.

In the wake of a failed audit, reporting requirements skyrocket. Controls, which are detailed reports of various types of activity that must be cross-checked for problems, may have to be run on a monthly or quarterly basis instead of annually. New controls are usually introduced. Other sorts of testing to discover problems will also usually result. The work related to all of this new activity must be staffed either from inside a company or by personnel from an auditing or consulting firm. Either way, costs rise.

A global reaction to improve governance

Everyone talks about Sarbanes-Oxley (SOX), but it's certainly not the only law shaping governance today. Numerous countries have enacted legislation to improve governance. As with the United States, many of these countries have passed legislation in response to the outcry over corporate scandals. Although they differ by name, the laws passed by various countries have similarities, namely with regard to establishing internal controls and effecting improved financial reporting:

- **Japan: J-SOX:** On June 7, 2006, Japanese legislators passed the Financial Instruments and Exchange Law, part of which includes the so-called J-SOX requirements. The two main components of the J-SOX legislation are the "Evaluation of and Reporting on Internal Control for Financial Reports," which forces management to assume responsibility for developing and operating internal controls, and the "Audit of Internal Control for Financial Reports," in which a company's external auditor, aside from its regular auditing duties, must conduct an audit of management's evaluation of the effectiveness of internal control for financial reports. The J-SOX requirements took effect starting in April 2008.
- **Canada: Bill 198:** Bill 198, also known as C-SOX, became effective on October 1, 2003. Its formal name is "Keeping the Promise for a strong Economy Act (Budget Measures), 2002." This bill requires companies to "[create and] maintain a system of internal controls related to the effectiveness and efficiency of their operations, including financial reporting and asset control." It also requires companies to place internal controls over their disclosure procedures.
- **Australia: CLERP 9 in Australia:** In 2001, Australia passed the Corporations Act, which governs corporate law. In 2004, a reform to the Corporations Act was passed, called the Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act 2004 (or CLERP 9). CLERP 9 aims to make sure that business regulation is consistent with promoting a strong economy, in addition to providing a framework that helps businesses adapt to change. Three entities were created by CLERP 9: The Financial Reporting Council, the Australian Stock Exchange's Corporate Governance Council, and the Shareholder and Investors Advisory Council.