SAP® GRC FOR DUMMIES®

by Denise Vu Broady and Holly A. Roland

Wiley Publishing, Inc.

SAP® GRC FOR DUMMIES®

by Denise Vu Broady and Holly A. Roland

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

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

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

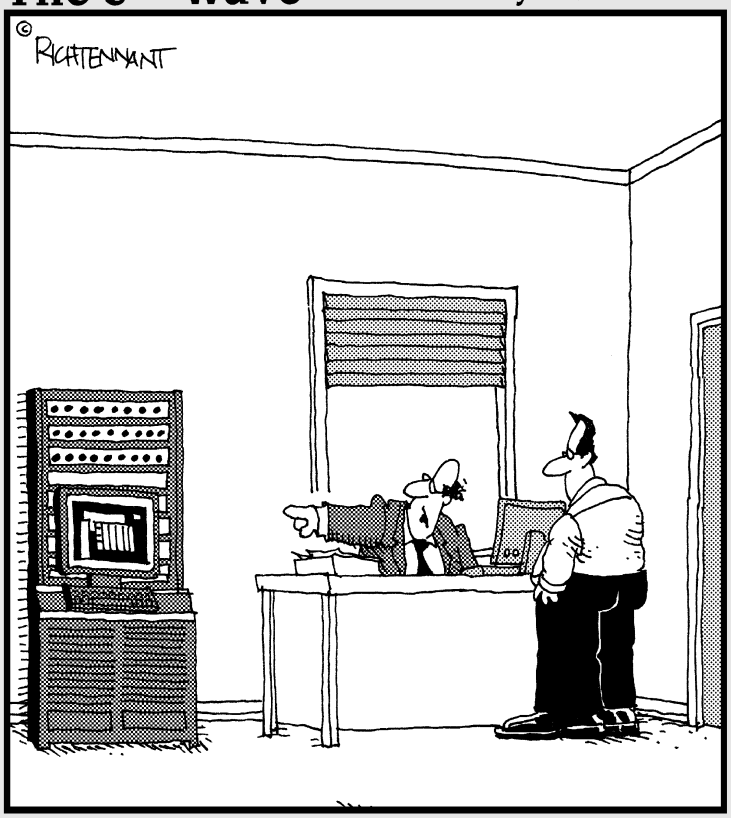
If you're new to SAP GRC or GRC in general, your next step is to head straight to Chapter 1, which gives you the ABCs of GRC, as well as providing food for thought about what GRC can do for you.

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.

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?