

Don't drown in GRC alphabet soup!  
Here's how to stay safe and sane

# SAP® GRC

## FOR DUMMIES®

**A Reference  
for the  
Rest of Us!®**

FREE eTips at [dummies.com](http://dummies.com)®

Denise Vu Broady  
Holly A. Roland

Remain compliant  
while you help  
your business  
grow



*Don't drown in GRC alphabet soup!  
Here's how to stay safe and sane*

# SAP® GRC

FOR

# DUMMIES®

*Remain compliant  
while you help  
your business  
grow*

*A Reference  
for the  
Rest of Us!®*

*FREE eTips at [dummies.com](http://dummies.com)®*

**Denise Vu Broady  
Holly A. Roland**



# ***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 St.

Hoboken, NJ 07030-5774

[www.wiley.com](http://www.wiley.com)

Copyright © 2008 by Wiley Publishing, Inc.,  
Indianapolis, Indiana

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317)

572-4355, or online at  
<http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

<p><b>LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY:</b> The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting,</p>
---

or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

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](http://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



# 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/](http://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](http://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

## Title

[Introduction](#)

[About This Book](#)

[Foolish Assumptions](#)

[How This Book Is Organized](#)

[Icons Used in This Book](#)

[Where to Go from Here](#)

## Part I : Governance, Risk, and Compliance Demystified

[Chapter 1: The ABCs of GRC](#)

[Getting to Know GRC](#)

[Getting in the Business Drivers' Seat](#)

[Getting Motivated to Make the Most of GRC](#)

[Introducing the GRC Stakeholders](#)

[Understanding GRC by the Letters](#)

[C Is for Compliance: Playing by the Rules](#)

[R Is for Risk: Creating Opportunity](#)

[G Is for Governance: Keeping Focused and Current](#)

[Hitting the Audit Trail](#)

[Designing Your Approach to GRC](#)

[What GRC Solutions Provide](#)

[Chapter 2: Risky Business: Turning Risks into Opportunities](#)

[Discovering Enterprise Risk Management](#)

[Defining Risk](#)

[Ignoring Risk \(At Your Peril\)](#)

[Sorting Through the Approaches to Risk Management](#)

[Identifying the Critical Components of a Successful Risk Management Framework](#)

[Taking the Four Steps to Enterprise Risk Management](#)

[Analyzing What Went Wrong: When Risk Becomes Reality](#)

[Automating the Risk Management Cycle](#)

[Taking the SAP Approach: SAP GRC Risk Management](#)

[Using SAP GRC Risk Management: A Fictional Case Study](#)

[Using SAP Risk Management: An SAP Case Study](#)

[Gleaning the Benefits of SAP GRC Risk Management](#)

[Chapter 3: Governance: GRC in Action](#)

[Getting to Know Governance](#)

[Gleaning the Benefits of Good Governance](#)

[Drafting Governance Blueprints](#)

[Creating a Framework for Great Governance](#)

[Evaluating Your Governance Framework](#)

[Hurdles to Instituting and Maintaining a Good Framework](#)

[Making the Argument for Automation](#)

[The SAP Approach: Integrated Holistic IT for GRC](#)

[Coming to Grips with Governance](#)

## [Part II : Diving into GRC](#)

[Chapter 4: How Sarbanes and Oxley Changed Our Lives](#)

[Figuring Out Whether SOX Applies to You](#)

[Discovering Why SOX Became Necessary](#)

[Who Are Sarbanes and Oxley, Anyway?](#)

[Breaking Down SOX to the Basics](#)

[Information Technology: SOX in a Box](#)

[Paying Up: What's SOX Going to Cost You?](#)

[Setting the Record Straight](#)

[Other Laws You Need to Know About](#)

[We're All In This Together: Convergence](#)

[Sorting Out the Benefits of SOX](#)

[Chapter 5: Fraud, Negligence, and Entropy: What Can Go Wrong and How to Prevent It](#)

[Defining Fraud](#)

[Negligence: More Likely Than Fraud](#)

[Entropy: Errors, Omissions, and Inefficiencies](#)

[Cleaning Up: The Mop-Up Operation](#)

[Chapter 6: Access Control and the Role of Roles](#)

[Understanding Access Control and Roles](#)

[Getting a Handle on Access Control](#)

[How Access Control Got Messy](#)

[Getting Clean](#)

[Staying Clean](#)

[Managing Exceptional Access](#)

[The SAP Approach: SAP GRC Access Control](#)

[Where Do You Go from Here?](#)

[Chapter 7: Taking Steps toward Better Internal Controls](#)

[Understanding Internal Controls](#)

[Exploring the Benefits of Better Controls](#)



[Seeing How Automating Controls Makes Things Easier](#)

[Taking Five Steps to Better Internal Controls](#)

[Getting to Know the SAP Approach: SAP GRC Process Control](#)

[Chapter 8: It's a Small World: Effectively Managing Global Trade](#)

[Understanding Four Reasons Why Global Trade Is So Complex](#)

[Figuring Out the Complexities of Importing](#)

[Making Sure You're Complying with All 19,391 Exporting Restrictions](#)

[Taking Advantage of the System: Trade Preference Management](#)

[Discovering the Different Ways to Manage Global Trade](#)

[Using the SAP Approach: SAP GRC Global Trade Services](#)

## [Part III : Going Green](#)

[Chapter 9: Making Your Company Environmentally Friendly](#)

[Discovering the Three Ps of Going Green: People, Processes, and Products](#)

[Going Green: It's Not Just for Tree-Huggers Anymore](#)

[Understanding Why Your Company Should Go Green](#)

[Going Green Is Good Business](#)

[Implementing Green Practices](#)

[Going Green Is also the Law](#)

[A Final Word About Going Green](#)

[Chapter 10: Keeping Employees Healthy and Safe](#)

[Keeping Your Employees Safe and Healthy: The Big Picture](#)

[Moving Down the Road to Zero Accidents](#)

[Making the Case for Automation and Integration](#)

[Taking the SAP Approach to Employee Health and Safety](#)

[Chapter 11: Making Your Business Processes Environmentally Friendly](#)

[Discovering Ways in which All Companies Can Go Green](#)

[Reducing Your Energy Use and Costs](#)

[Building, Renovating, and Cleaning with Sustainable Resources and Materials](#)

[Getting LEED Certified](#)

[Assessing Your Environmental Risks](#)

[Greening Manufacturing](#)

[Adopting Green Practices for Manufacturing](#)

[Taking the SAP Approach to Making Your Processes Environmentally Friendly](#)

[Chapter 12: Making Your Products Environmentally Friendly](#)

[Discovering What It Takes to Make Products Environmentally Friendly](#)

[Figuring Out What Your Materials Are and What They Do](#)

[Realizing the Benefits of Compliance](#)

[Using Hazardous Materials Responsibly](#)

[Working with Hazardous Materials](#)

[Keeping Up with Materials Legislation](#)

[Exploring the SAP Approach to Product Compliance](#)

## [Part IV : Managing the Flow of Information](#)

[Chapter 13: Sustainability and Corporate Social Responsibility](#)

[Discovering the Great Power and Responsibility of Big Companies](#)

[Getting the Lowdown on Sustainability](#)

[Discovering Why Sustainability Is Good Business](#)

[Discovering the Possible Downside of CSR](#)

[Managing Sustainability Performance](#)

[Discovering Why an Automated Solution Is Needed](#)

## Chapter 14: IT GRC

Getting a Handle on What IT GRC Is

Understanding IT Governance in Terms of Risk and Compliance

Securing Your Software Applications

Keeping the Kimono Closed: Data Privacy

Protecting Key Corporate Assets: Intellectual Property

## Chapter 15: Turning On the Lights with GRC and CPM

Turning On the Lights with CPM

Making the Case for CPM and GRC Integration

Seeing CPM and GRC Integration in Practice

Discovering the Reusable Technology of GRC

## Part V : The Part of Tens

### Chapter 16: Top Ten GRC Strategies

Evaluate Which of the Most Prevalent GRC Issues Apply to You

Adopt Best Practices

Implement Key GRC Strategies

Set Yourself Up for Success

Watch Out for Danger Signs

Define GRC Roles and Responsibilities

Shake Down the People Who Know

Move to Strategic Adoption of Automated Controls

Adopt Strategies for Cleaning Up Access Control

Getting Your GRC Project Going and Keeping It Going

### Chapter 17: Ten Best Practices in Global Trade

Automate or Else

[Don't Go to Pieces](#)

[Make Sure You Can Trust Your Partners](#)

[Avoid Importing Delays](#)

[Get On Board with the Government's High-Tech Documenting Processes](#)

[Know Who Is Allowed at the Party](#)

[Know Who You're Shipping to](#)

[Get the Right Licenses](#)

[Take the Free Money](#)

[Leave a Paper Trail](#)

[Chapter 18: Ten Groups of GRC Thought Leadership Resources](#)

[GRC Resources](#)

[Risk Resources](#)

[SOX Resources](#)

[Financial Compliance Resources](#)

[Access Control and Process Control Resources](#)

[IT GRC Resources](#)

[Global Trade Resources](#)

[Employee Health and Safety Resources](#)

[Going Green Resources](#)

[Sustainability Resources](#)

[Glossary](#)

# Introduction

---

**G**RC 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.