

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

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.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: 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, 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.

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/.

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

<i>Introduction</i>	1
<i>Part I: Governance, Risk, and Compliance Demystified</i>	7
Chapter 1: The ABCs of GRC	9
Chapter 2: Risky Business: Turning Risks into Opportunities.....	39
Chapter 3: Governance: GRC in Action.....	67
<i>Part II: Diving into GRC</i>	87
Chapter 4: How Sarbanes and Oxley Changed Our Lives	89
Chapter 5: Fraud, Negligence, and Entropy: What Can Go Wrong and How to Prevent It.....	105
Chapter 6: Access Control and the Role of Roles.....	115
Chapter 7: Taking Steps toward Better Internal Controls	127
Chapter 8: It's a Small World: Effectively Managing Global Trade	141
<i>Part III: Going Green</i>	157
Chapter 9: Making Your Company Environmentally Friendly	159
Chapter 10: Keeping Employees Healthy and Safe.....	173
Chapter 11: Making Your Business Processes Environmentally Friendly	189
Chapter 12: Making Your Products Environmentally Friendly	217
<i>Part IV: Managing the Flow of Information</i>	243
Chapter 13: Sustainability and Corporate Social Responsibility	245
Chapter 14: IT GRC	265
Chapter 15: Turning On the Lights with GRC and CPM	281
<i>Part V: The Part of Tens</i>	295
Chapter 16: Top Ten GRC Strategies	297
Chapter 17: Ten Best Practices in Global Trade.....	305
Chapter 18: Ten Groups of GRC Thought Leadership Resources	309
<i>Glossary</i>	321
<i>Index</i>	331

Table of Contents

.....

<i>Introduction</i>	1
About This Book.....	1
Foolish Assumptions	2
How This Book Is Organized.....	2
Part I: Governance, Risk, and Compliance Demystified	3
Part II: Diving into GRC	3
Part III: Going Green	3
Part IV: Managing the Flow of Information.....	3
Part V: The Part of Tens.....	4
Glossary.....	4
Icons Used in This Book.....	4
Where to Go from Here.....	5

Part 1: Governance, Risk, and Compliance Demystified7

Chapter 1: The ABCs of GRC	9
Getting to Know GRC	9
Getting in the Business Drivers' Seat	11
Getting Motivated to Make the Most of GRC	14
Complying with financial regulations	14
Failing an audit	15
Experiencing a rude awakening.....	17
Going from private to public.....	17
Managing growth	18
Taking out an insurance policy.....	19
Managing risk.....	19
Reducing costs.....	19
Struggling with the high volume of compliance.....	20
Introducing the GRC Stakeholders.....	20
GRC stakeholders inside a company	21
GRC stakeholders outside a company.....	21
Understanding GRC by the Letters	22
Governance	23
Risk.....	23
Compliance	23
C Is for Compliance: Playing by the Rules	25
Controls: Mechanisms of compliance.....	25
Domains of compliance	27
R Is for Risk: Creating Opportunity.....	30
G Is for Governance: Keeping Focused and Current.....	31
Hitting the Audit Trail.....	32



Designing Your Approach to GRC33
 After the rush to clean up33
 Stages of GRC adoption34
What GRC Solutions Provide35

Chapter 2: Risky Business: Turning Risks into Opportunities 39

Discovering Enterprise Risk Management39
Defining Risk40
Ignoring Risk (At Your Peril).....42
Sorting Through the Approaches to Risk Management43
 The ad hoc approach.....43
 The fragmented approach.....43
 The risk manager’s job approach.....46
 The systematic, enterprise-wide approach46
 A cultural approach47
Identifying the Critical Components of a Successful
 Risk Management Framework.....47
 A culture that takes risk seriously, from the C-suite down48
 A risk management organization: Distributing
 responsibility throughout the culture50
 A systematic framework in place52
 Technology that creates a risk picture53
Taking the Four Steps to Enterprise Risk Management53
 Risk planning.....54
 Risk identification and analysis55
 Risk response.....56
 Risk monitoring57
Analyzing What Went Wrong: When Risk Becomes Reality57
Automating the Risk Management Cycle58
Taking the SAP Approach: SAP GRC Risk Management58
 SAP GRC risk management and key risk indicators59
 Monitoring risks and key risk indicators with
 SAP GRC Risk Management60
Using SAP GRC Risk Management: A Fictional Case Study61
 Where should we produce?.....62
Using SAP Risk Management: An SAP Case Study63
Gleaning the Benefits of SAP GRC Risk Management64

Chapter 3: Governance: GRC in Action 67

Getting to Know Governance.....67
Gleaning the Benefits of Good Governance69
Drafting Governance Blueprints.....70
Creating a Framework for Great Governance71
Evaluating Your Governance Framework.....76
 From a strategic and operational perspective76
 From a legal and regulatory compliance perspective77

Hurdles to Instituting and Maintaining a Good Framework78
 Avoiding GRC silos79
 Making GRC strategic.....79
 Justifying the cost of GRC80
 Applying GRC too narrowly.....81
 Setting up checks and balances82
 Making the Argument for Automation.....82
 The SAP Approach: Integrated Holistic IT for GRC.....83
 Coming to Grips with Governance.....85

Part II: Diving into GRC.....87

Chapter 4: How Sarbanes and Oxley Changed Our Lives89

Figuring Out Whether SOX Applies to You90
 Discovering Why SOX Became Necessary.....91
 Who Are Sarbanes and Oxley, Anyway?92
 Breaking Down SOX to the Basics.....93
 Sections 302 and 906: Threatening management
 with a big stick93
 Section 404: Ensuring a healthy immune system96
 What does Section 404 mean for business?97
 Information Technology: SOX in a Box.....98
 IT frameworks: Your template for compliance99
 COSO’s control framework.....99
 The SOX ripple effect100
 Paying Up: What’s SOX Going to Cost You?100
 SOX Costs Then100
 SOX Costs Now101
 Setting the Record Straight101
 Other Laws You Need to Know About102
 We’re All In This Together: Convergence102
 Japan’s J-SOX102
 Australia’s CLERP-9103
 Canada’s C-11103
 Basel II.....103
 Sorting Out the Benefits of SOX103

**Chapter 5: Fraud, Negligence, and Entropy:
 What Can Go Wrong and How to Prevent It105**

Defining Fraud106
 Motivations for fraud107
 Sowing the seeds of fraud107
 Some common examples of fraud108
 The Barings Bank scandal: Operations risk extraordinaire109

Negligence: More Likely Than Fraud	111
Entropy: Errors, Omissions, and Inefficiencies	111
Cleaning Up: The Mop-Up Operation.....	112
Thinking like an auditor.....	113
Making the computer your auditor.....	113

Chapter 6: Access Control and the Role of Roles115

Understanding Access Control and Roles.....	115
Getting a Handle on Access Control	116
Users and permissions	117
The roles revolution.....	118
How Access Control Got Messy	118
Every user is different.....	118
Virtual things are hard to track	119
IT and business don't speak the same language	119
Exceptional circumstances dictate exceptional access	120
Large scale increases complexity.....	120
Getting Clean	121
Figuring out where you stand	121
Staying Clean	123
Managing Exceptional Access	124
The SAP Approach: SAP GRC Access Control	125
Where Do You Go from Here?	126

Chapter 7: Taking Steps toward Better Internal Controls127

Understanding Internal Controls	127
Exploring the Benefits of Better Controls	128
Benefit one: Business process improvement.....	129
Benefit two: Management by exception	129
Benefit three: Real-time monitoring.....	129
Benefit four: Mindset changes	131
Seeing How Automating Controls Makes Things Easier.....	131
Taking Five Steps to Better Internal Controls.....	134
Documentation: The mapping exercise.....	134
Testing: Real-time and historical	135
Remediation: Fixing the problem	135
Analysis: Reports for management	135
Optimization: Barring risk.....	136
Getting to Know the SAP Approach: SAP GRC Process Control.....	136
Single system of record	136
Continuous monitoring.....	137
Out-of-the-box monitoring.....	137
End-to-end internal controls	138

Chapter 8: It’s a Small World: Effectively Managing Global Trade141

- Understanding Four Reasons Why Global Trade Is So Complex142
 - Long supply chains143
 - New regulations and security initiatives144
 - Modernization of government IT systems145
 - Increasing complexity of regulations146
- Figuring Out the Complexities of Importing148
 - Classifying an item: What is it?148
 - Making way for the goods: Pre-clearance149
 - Making it through: Clearing Customs149
 - Reconciling value: The step most often missed149
 - Getting the lead out: Brand protection.....150
- Making Sure You’re Complying with All 19,391
 - Exporting Restrictions150
 - Knowing who you’re dealing with150
 - Obtaining the right export licenses151
 - Knowing how the product will be used152
- Taking Advantage of the System: Trade Preference Management.....153
- Discovering the Different Ways to Manage Global Trade153
- Using the SAP Approach: SAP GRC Global Trade Services.....154

Part III: Going Green 157

Chapter 9: Making Your Company Environmentally Friendly159

- Discovering the Three Ps of Going Green: People, Processes, and Products160
- Going Green: It’s Not Just for Tree-Huggers Anymore.....161
- Understanding Why Your Company Should Go Green162
- Going Green Is Good Business.....164
 - Enhance your image.....164
 - Build trust with regulatory authorities166
 - Influence future events166
- Implementing Green Practices167
 - Trees matter167
 - Let there be (green) light!.....167
 - Water: To bottle or not to bottle?.....168
 - Reduce your risk168
- Going Green Is also the Law.....169
 - Compliance169
 - Risks of noncompliance: Fines and public relations nightmares170
- A Final Word About Going Green171

Chapter 10: Keeping Employees Healthy and Safe173

Keeping Your Employees Safe and Healthy: The Big Picture	174
Enabling and maintaining good health	175
Avoiding accidents	175
Healthy benefits equal employee recruitment retention	176
Moving Down the Road to Zero Accidents	177
Organizing and managing a comprehensive health and safety program.....	177
Assessing risks.....	178
Standardizing your procedures	179
Managing accidents	180
Inspecting your sites and creating new safety measures.....	181
Educating your employees	182
Making the Case for Automation and Integration.....	183
Taking the SAP Approach to Employee Health and Safety	184
The Occupational Health module	184
The Industrial Hygiene and Safety module	185

**Chapter 11: Making Your Business Processes
Environmentally Friendly189**

Discovering Ways in which All Companies Can Go Green	190
Reducing Your Energy Use and Costs.....	190
Building, Renovating, and Cleaning with Sustainable Resources and Materials	192
Begin at the beginning with green design	192
Pick the right spot	192
Crunch your numbers.....	193
Make friends with your site plan.....	193
Reduce unnecessary strains on your HVAC.....	194
Exploit the advantages of technology	194
Command the water.....	194
Use green and recycled building materials	194
Build smart, build green	196
Renovate green	196
Clean green.....	196
Recycle.....	197
Reducing travel.....	198
Getting LEED Certified	198
Assessing Your Environmental Risks	201
Greening Manufacturing.....	202
Green legislation	202
EPA Clean Air Act.....	203
EPA Clean Water Act.....	204
Waste Electrical and Electronic Equipment (WEEE).....	206
Adopting Green Practices for Manufacturing.....	208
Establish an energy management program.....	208
Reduce emissions.....	209
Reduce waste	210

Deal with hazardous substances210
 Optimize occupational health210
 Promote industrial hygiene and safety.....211
 Ensure product safety.....211
 Taking the SAP Approach to Making Your Processes
 Environmentally Friendly211
 SAP Environmental Compliance212
 SAP Waste Management: A core component of
 SAP Environment, Health, and Safety.....215

Chapter 12: Making Your Products Environmentally Friendly217

Discovering What It Takes to Make Products
 Environmentally Friendly218
 Figuring Out What Your Materials Are and What They Do219
 Defining hazardous materials220
 Defining dangerous goods.....221
 Realizing the Benefits of Compliance222
 The benefits of complying.....223
 The risks of failing to comply224
 Using Hazardous Materials Responsibly.....225
 Customer compliance management226
 Supplier compliance management226
 Compliance reporting.....226
 Comprehensive task management226
 Working with Hazardous Materials.....227
 Packing.....227
 Materials communications.....228
 Transporting materials.....228
 Keeping Up with Materials Legislation.....229
 Toxic Substances Control Act (TSCA)229
 Registration, Evaluation, Authorization of
 Chemicals (REACH).....230
 Reduction of Hazardous Substances (RoHS).....234
 Exploring the SAP Approach to Product Compliance235
 Compliance for Products by TechniData (CiP)236
 SAP EH&S.....238

Part IV: Managing the Flow of Information243

Chapter 13: Sustainability and Corporate Social Responsibility .. 245

Discovering the Great Power and Responsibility of Big Companies246
 Getting the Lowdown on Sustainability247
 Discovering Why Sustainability Is Good Business.....250
 Managers recognize sustainability as a top priority250
 Stakeholders exert pressure251
 Sustainable businesses have better access to capital.....253
 Government regulations increasingly require it.....254

Sustainability helps you manage risk	254
CSR protects your brand image.....	255
It helps you attract and keep the best employees	256
CSR is ethical	256
It helps business planning and innovation	256
CSR increases profits	257
Discovering the Possible Downside of CSR	258
Managing Sustainability Performance.....	258
The current reporting process is a mess	259
New tactics are required	259
Discovering Why an Automated Solution Is Needed	260
Sustainability reporting is a recurring problem	260
Huge amounts of data are involved	260
Integration is a plus.....	261
Automation creates supply chain transparency	261
Automation means auditability	262
Automation yields analytics and benchmarks	262
An IT solution speeds distribution of data	263
Chapter 14: IT GRC	265
Getting a Handle on What IT GRC Is	266
Understanding IT Governance in Terms of Risk and Compliance	267
In terms of risk.....	268
In terms of compliance	269
Keeping up with the pace of change.....	271
Securing Your Software Applications	272
Taking basic application security measures.....	272
Consolidating security solutions.....	273
Making friends with the IT department.....	274
Keeping the Kimono Closed: Data Privacy	275
Protecting Key Corporate Assets: Intellectual Property.....	276
Cinching Up the Kimono.....	276
Leveraging the network.....	277
Other ways data can walk away	278
Protecting IT assets.....	279
Communication	280
Chapter 15: Turning On the Lights with GRC and CPM	281
Turning On the Lights with CPM.....	282
Making the Case for CPM and GRC Integration.....	284
Understanding obstacles to integration.....	285
Instrumenting the enterprise.....	286
Collecting the payoff from CPM and GRC integration	287
Supplier concentration	288
Loan processing.....	289

Seeing CPM and GRC Integration in Practice.....289
 The intersection of actuals289
 Strategy, risk, and planning.....290
 Governance and strategy290
 Discovering the Reusable Technology of GRC291
 Repository.....291
 Document management.....291
 Case management292
 Workflow.....292
 Process modeling292
 Policy engine.....292
 Rule engine.....293
 Controls293
 Reporting.....293
 Standardized interfaces to components293
 Composite apps on the platform.....294

Part V: The Part of Tens295

Chapter 16: Top Ten GRC Strategies297

Evaluate Which of the Most Prevalent GRC Issues Apply to You297
 Adopt Best Practices298
 Implement Key GRC Strategies.....299
 Set Yourself Up for Success299
 Watch Out for Danger Signs.....299
 Define GRC Roles and Responsibilities300
 Shake Down the People Who Know301
 Move to Strategic Adoption of Automated Controls302
 Adopt Strategies for Cleaning Up Access Control302
 Getting Your GRC Project Going and Keeping It Going303

Chapter 17: Ten Best Practices in Global Trade305

Automate or Else.....305
 Don't Go to Pieces.....305
 Make Sure You Can Trust Your Partners306
 Avoid Importing Delays.....306
 Get On Board with the Government's High-Tech
 Documenting Processes306
 Know Who is Allowed at the Party307
 Know Who You're Shipping to.....307
 Get the Right Licenses.....307
 Take the Free Money.....307
 Leave a Paper Trail308

Chapter 18: Ten Groups of GRC Thought Leadership Resources . . . 309

GRC Resources	309
Web sites	309
Blogs.....	310
Online journals	310
Risk Resources	311
Web sites	311
Blogs.....	311
Books	311
SOX Resources	312
Web sites and forums.....	312
Books	312
Financial Compliance Resources	312
J-SOX	313
Basel II.....	313
Foreign Corrupt Practices Act	313
Access Control and Process Control Resources	314
Web sites	314
Articles.....	314
Wikis.....	314
IT GRC Resources.....	315
Blogs.....	315
Global Trade Resources	315
Web sites	315
Blogs.....	316
Employee Health and Safety Resources	316
Web sites and online journals.....	317
Blogs.....	317
Articles.....	317
Going Green Resources	317
Web sites	317
Wikis.....	318
Articles.....	318
Blogs.....	319
Books	319
Sustainability Resources	319
Web sites	319
Articles.....	320
Blogs and books	320

***Glossary*** **321**

***Index*.....** **331**

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.

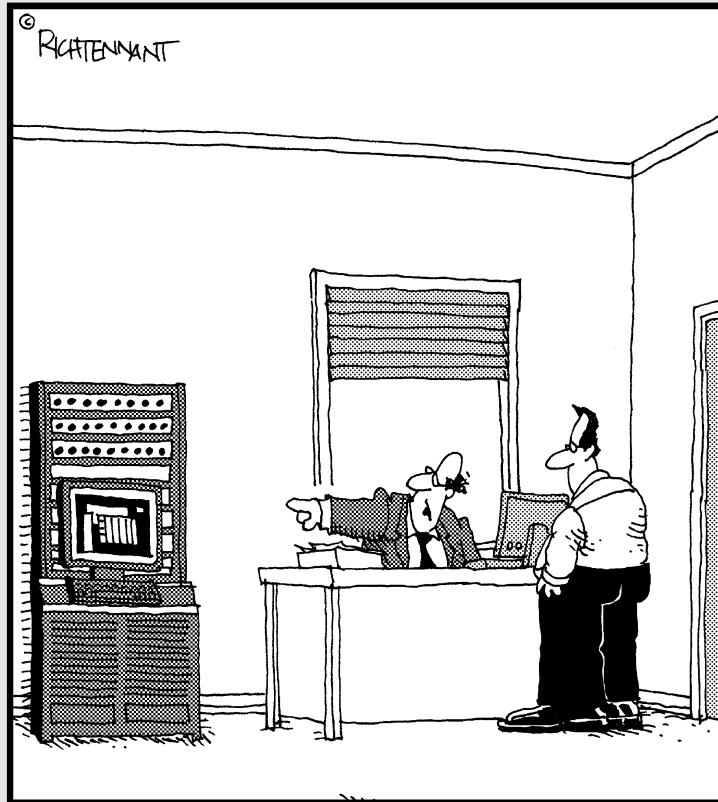
If you're a professional in a particular area — such as global trade, risk management, or IT governance — you could decide to visit particular chapters in no particular order. But (and we're probably biased) we think the best way forward from here is straight into Chapter 1 (with a few intervening pages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