

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 Demystified 7

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 approach43
 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 extraordinaire.....109

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 Green157

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 goods221
 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 reporting226
 Comprehensive task management226
 Working with Hazardous Materials227
 Packing.....227
 Materials communications228
 Transporting materials228
 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 to307
 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***321Index*.....**331