Index

Accounts Payable Process Review Procedures
  SOx Section 404 Internal Controls Assessments, 191
Actions to Resolve Risks
  COSO ERM Control Activities, 97
Activity Management
  COSO ERM Control Activities, 81
AICPA SAS No. 1
  Internal Controls Definition, 148
AICPA SAS No. 55
  Internal Controls Definition, 154
Air 21 Statute
  U.S. Federal Whistleblower Rules, 205
Annual Audit Plans
  COSO ERM, 251
Application Development and Acquisition Risks
  Information Technology and Enterprise Risk Management, 295
  Purchased Software Contract Guidelines, 299
  SDLC Risks, 297
  SDLC Waterfall Model, 296
Application Systems Risks
  Application Systems Testing, 300
  ERP Software Application Risks, 298
  Information Technology and Enterprise Risk Management, 292
  In-House Developed Software, 298
Application Systems Testing
  Application Systems Risks, 300
Arthur Andersen
  Enron and WorldCom Corporate Debacles, 178
AS5 Risk-Based Auditing Standards
  Sarbanes-Oxley Act (SOx), 198
AS 8 through AS 15
  PCAOB Risk Standards, 200
Assessing Selected Process Risks
  SOx Section 404 Internal Controls Assessments, 190
Assignment of Authority and Responsibility
  Control Environment Factors, 11
  COSO ERM Components, 59
Audit Committee and Risk Committee Coordination
  Board of Directors Responsibilities, 244
Audit Committee Charters
  Audit Committees, 237
Audit Committee Functions and Responsibilities
  Board of Directors Responsibilities, 237
Audit Committees
  Audit Committee Charters, 237
  Board of Directors Responsibilities, 234
Auditable Entities
  Ranking Internal Audit Risks, 260

Bayer Group
  Corporate Compliance Statement, 135
Benchmarking
  Risk Monitoring, 86
Bhopal India
  Risk Events, 42
  Union Carbide Bhopal India Risk Event, 42
Board Committee Structure
  Board of Directors Responsibilities, 233
Board of Directors and the Audit Committee
  Control Environment Factors, 9
  COSO Internal Controls Control Environment, 161

COPYRIGHTED MATERIAL

http://www.pbookshop.com

- Board of Directors Responsibilities
  - Audit Committee and Risk Committee Coordination, 244
  - Audit Committee Functions and Responsibilities, 237
  - Audit Committees, 234
  - Board Committee Structure, 233
  - Corporate Charters, 231
  - COSO ERM, 228
  - Enterprise governance, 128
  - GRC Principles, 228
  - Risk Committee Board Member Requirements, 242
  - Risk Committees, 238
  - Risk Oversight Responsibilities, 233
  - Sarbanes-Oxley Act (SOx), 225
- Board of Directors' Attitudes
  - COSO ERM Components, 57
- Board or Senior Management Risk Concerns
  - Risk Assessment Reviews, 112
- Brainstorming Approaches
  - Risk Identification, 36
- Building a GRC Culture
  - GRC Education Programs, 326
- Building a Project Management Organization
  - Project Management Processes, 288
- Burgundy Book
  - OCEG Capability Model, 223
- Business Continuity Plan Requirements
  - IT General and Application Controls, 305
- Business Continuity Plans (BCPs)
  - IT Continuity Planning, 304
- Chief Risk Officer (CRO)
  - Establishing an Effective Risk Management Function, 90
- Chief Risk Officer (CRO) Position Description
  - Effective Enterprise Risk Management, 94
  - Establishing an Effective Risk Management Function, 93
- Code acknowledgement requirement
  - Codes of Conduct, 125
- Codes of Conduct
  - Code Acknowledgement Requirement, 125
  - Enterprise Governance, 122
  - Ethical Business Practices, 122
- Commitment to Competence
  - Control Environment Factors, 8
  - COSO ERM Components, 58
  - COSO Internal Controls Control Environment, 160
- Communications and Information
  - COSO Internal Control Elements, 167
- Communications Aspects
  - COSO Internal Controls Framework, 169
- Communications to Stakeholders
  - Enterprise Governance Concepts, 124
  - Establishing of Enterprise-Wide Governance Awareness, 325
- Compliance Architectures Considerations
  - Enterprise Compliance, 28
- Compliance Issues Today
  - Corporate Governance in the United States, 132
- Compliance Policies
  - Effective Compliance Programs, 134
- Compliance Risk Assessments
  - Effective Compliance Programs, 137
- Compliance Self-Audits
  - Work Unit–Level Compliance Tracking, 141
- Compliance-Related Laws
  - Enterprise compliance, 140
- Compliance-Related Operational Procedures
  - Effective Compliance Programs, 134
- Compliance-Related Requirements
  - GRC Best Practices, 131
- Conduct Typical Topic Areas
  - Control Environment Factors, 7
- Content Management
  - Risk Awareness Guidelines, 101
- Continuous Risk Monitoring
  - Establishing an Effective Risk Management Function, 98
- Continuous Risk Monitoring
  - Risk Action Plans, 99
- Control Activities
  - COSO ERM Components, 78

http://www.pbookshop.com

Control Activities
  COSO Internal Control Elements, 166
Control Environment
  COSO Internal Control Elements, 5
Control Environment
  COSO Internal Control Elements, 159
Control Environment Factors
  Assignment of Authority and Responsibility, 11
Control Environment Factors
  Board of Directors and the Audit Committee, 9
Control Environment Factors
  Commitment to Competence, 8
Control Environment Factors
  Conduct Typical Topic Areas, 7
Control Environment Factors
  Human Resources Policies and Practices, 11
Control Environment Factors
  Integrity and Ethical Values, 6
Control Environment Factors
  Management’s Philosophy and Operating Style, 9
Control Environment Factors
  Organization Structure, 10
Control Materials Reviews
  Risk Monitoring, 85
Cooking the Books
  Enron and WorldCom Corporate Debacles, 178
Corporate Audit Committees
  Enterprise Governance, 119
Corporate Charters
  Board of Directors Responsibilities, 231
Corporate Compliance Statement
  Bayer Group, 135
Corporate Culture
  Risk Portfolio Management, 210
Corporate Governance
  COSO ERM, 244
Corporate Governance in the United States
  Compliance Issues Today, 132
  Enterprise Governance Background, 119
Corporate Responsibility for Financial Reports
  SOx Section 302, 193
Corporate Risks Summary
  COSO ERM Components, 63
  Global Computer Products Example Company, 18
COSO Definition of Internal Control
  COSO Internal Controls Framework, 4
COSO ERM
  Annual Audit Plans, 251
  Board of Directors Responsibilities, 228
  Corporate Governance, 244
  Defining the Risk Management Philosophy, 315
  Effective Internal Audit Planning, 255
  GRC Risk Management, 25
  IIA Risk Management Standards, 250
  Internal Audit Planning, 251
  IT General and Application Controls, 293
  Risk Based Internal Audits, 248
  Sarbanes-Oxley Act (SOx), 177
COSO ERM Application Techniques
  COSO ERM Guidance Material,69
  Information and Communication Flows, 82
  Loss Event Data Tracking, 70
  Risk Likelihood and Impact Mapping, 70
COSO ERM Components
  Assignments of Authority and Responsibility, 59
  Board of Directors’ Attitudes, 57
  Commitment to Competence, 58
  Control Activities, 78
  Corporate Risks Summary, 63
  Emerge Compliance and Risk Management Statement, 61
  Event Identification, 66
  External Economic Events, 67
  Human Resource Standards, 59
  Information and Communication, 81
  Integrity and Ethical Values, 57
  Internal Environment, 56
  Internal Infrastructure Events, 68
  Mission Statements, 62
  Objective Setting, 62
  Risk Acceptance, 75
  Risk Appetite, 57
  Risk Appetite Map, 61
  Risk Assessment, 71

http://www.pbookshop.com

COSO ERM Components (*Continued*)
  Risk Avoidance, 74
  Risk Management Philosophy, 56
  Risk Monitoring, 84
  Risk Reduction, 75
  Risk Sharing, 75
COSO ERM Control Activities
  Actions to Resolve Risks, 97
  Activity Management, 81
  ERM Activity Scope, 96
  Gramm-Leach-Bliley Act (GLBA), 95
  Information and Communication Flows, 79
  Information Processing, 81
  Performance Indicators, 81
  Risk Assessment Process, 79
  Risk Assessment Review and Internal Audit Report Comparison, 109
  Segregation of Duties, 81
COSO ERM Framework
  Definition Enterprise Risk Management, 53
  Enterprise Risk Management Definition, 53
  ERM Definitions and Objectives, 53, 55
  Portfolio View of Risk, 51
  Risk Objective Setting Components, 64
COSO ERM Guidance Material
  COSO ERM Application Techniques, 69
  Event Inventories, 69
  Facilitated Workshops, 69
  Process Flow Analysis, 69
  Risk Response Planning, 73
COSO ERM Risk Assessment Process
  Portfolio View of Risk, 77
  Risk Likelihood and Impact Mapping, 74
COSO Internal Control Elements
  Communications and Information, 167
  Control Activities, 166
  Control Environment, 5, 159
  Integrity and Ethical Values, 159
  Monitoring, 170
  Risk Assessment, 13, 164
  Risk Assessment as a Three-Step Process, 13
  Risk Assessment Process, 165
  COSO Internal Controls Framework, 5
COSO Internal Control Environment Factors
  Integrity and Ethical Values, 6
COSO Internal Control Monitoring
  Internal Control Evaluations, 172
COSO Internal Controls
  COSO Internal Controls Background, 149
  COSO Internal Controls Framework, 157
  Integrating COSO ERM, 148
COSO Internal Controls Background
  COSO Internal Controls, 149
  Foreign Corrupt Practices Act of 1977 (FCPA), 149
  Minahan Committee, 154
  SEC 1979 Internal Control Reporting Proposal, 153
  Treadway Commission, 151
COSO Internal Controls Control Environment
  Board of Directors and the Audit Committee, 161
  Commitment to Competence, 160
  Human Resources Policies and Practices, 163
  Management's Philosophy and Operating Style, 161
COSO Internal Controls Framework
  Communications Aspects, 169
  COSO Definition of Internal Control, 4
  COSO Internal Control Environment, 5
  COSO Internal Controls, 157
  Internal Controls Background, 2
  National Commission on Fraudulent Financial Reporting, 3
  Quality of Information, 168
  Strategic and Integrated Systems, 167
  Treadway Commission, 2
COSO Internal Controls Report
  Definition of Internal Controls, 3
  Internal Control–Integrated Framework, 3
CRO Responsibilities
  Establishing an Effective Risk Management Function, 91

http://www.pbookshop.com

- Dashboard Monitoring Tools
  - Risk Monitoring, 66, 84
- Decision Tree Analysis
  - Quantitative Risk Analysis, 49
- Defining the Risk Management Philosophy
  - COSO ERM, 315
  - Relative Risks versus Expected Returns, 318
- Definition of Enterprise Risk Management
  - COSO ERM framework, 53
- Definition of Internal Controls
  - COSO Internal Controls Report, 3
- Definition of Project Management
  - Project Management Processes, 267
- Delphi Method
  - Quantitative Risk Analysis, 45
- Dow Chemical Risk Event
  - Risk Events, 42

- Effective Compliance Programs
  - Compliance Policies, 134
  - Compliance Risk Assessments, 137
  - Compliance-Related Operational Procedures, 134
- Effective Compliance Programs
  - Enterprise Compliance, 134
  - Enterprise Compliance Issues, 144
  - Enterprise Rules versus Compliance Options, 136
  - Internal Audit Compliance Reviews, 139
  - Work Unit–Level Compliance Tracking, 139
- Effective Continuity Planning
  - Information Technology and Enterprise Risk Management, 292
- Effective Enterprise Risk Management
  - Chief Risk Officer (CRO) Position Description, 94
  - Legal and Regulatory Risks, 108
  - Policies and Standards, 103
  - Risk Activity Scope, 97
  - Risk Assessment Reviews, 111
  - Risk Management Organizations, 101
  - Risk Management Policies and Standards, 100
  - Risk-Awareness Cultures, 100
- Effective ERM Processes
  - IT General and Application Controls, 309
- Effective GRC Principles
  - Governance, Risk, and Compliance Principles, 22
- Effective Internal Audit Planning
  - COSO ERM, 255
- Effectiveness of the Internal Control Structure Reports
  - SOx Section 404 Internal Controls Assessments, 192
- Emerge Compliance and Risk Management Statement
  - COSO ERM Components, 61
- Enron and WorldCom Corporate Debacles
  - Arthur Andersen, 178
  - Cooking the books, 178
  - Enterprise Governance Background, 119
  - Enterprise Risk Management Concerns, 178
- Enterprise Business Risks
  - Likelihood and Relative Significance Assessments, 37
  - Risk Assessment Analysis, 38
  - Risk Management Fundamentals, 35
- Enterprise Codes of Conduct
  - Establishing of Enterprise-Wide Governance Awareness, 324
- Enterprise Compliance
  - Compliance Architectures Considerations, 28
  - Compliance-Related Laws, 140
  - Effective Compliance Programs, 134
  - Enterprise Compliance Hotlines, 143
  - Establishing a Compliance Assessment Team, 133
  - GRC Concepts, 26
  - Management Compliance Reviews, 142
  - Risk Assessment Matrix, 138
  - U.S. Department of Labor Compliance-Related Laws, 140
  - Whistleblower Programs, 143
- Enterprise Compliance Hotlines
  - Enterprise Compliance, 143
- Enterprise Compliance Issues
  - Effective Compliance Programs, 144

http://www.pbookshop.com

Enterprise Governance
  Board of Directors Responsibilities, 128
  Codes of Conduct, 122
  Corporate Audit Committees, 119
  Ethical Behavior and Integrity, 119
  Ethics Functions, 119
Enterprise Governance Background
  Corporate Governance in the United States, 119
  Enron and WorldCom Corporate Debacles, 119
  Foreign Corrupt Practices Act (FCPA), 118
  Watergate Scandal, 117
Enterprise Governance Concepts
  Communications to Stakeholders, 124
  GRC Practices, 116
  Mission Statements, 120
  Principal Agent Model, 117
  Rights and Equitable Treatment of Shareholders, 127
  Roles and Responsibilities of the Board of Directors, 129
Enterprise Governance Practices
  Governance, Risk and Compliance, 15
Enterprise GRC programs
  Management Compliance Reviews, 144
Enterprise Objectives
  Establishing an Effective GRC Culture, 312
  Promoting Enterprise Risk Concepts, 314
Enterprise Risk Awareness Programs
  Risk Assessment Reviews, 112
Enterprise Risk Management
  SOx Section 404 Internal Controls Assessments, 193
Enterprise Risk Management Concerns
  Enron and WorldCom corporate debacles, 178
  Sarbanes-Oxley Act (SOx), 178
Enterprise risk management definition
  COSO ERM Framework, 53
  ERM Processes, 53
Enterprise Risk Management Guidance
  National Institute of Science and Technology (NIST), 211
Enterprise Risk Model Framework
  Risk Management Fundamentals, 34
Enterprise Risk Organization Responsibilities
  Establishing an Effective Risk Management Function, 91
Enterprise Rules versus Compliance Options
  Effective Compliance Programs, 136
ERM Activity Scope
  COSO ERM Control Activities, 96
ERM Definitions and Objectives
  COSO ERM Framework, 53, 55
  Risk Appetite, 54
ERM Processes
  Enterprise Risk Management Definition, 53
ERP Software Application Risks
  Application Systems Risks, 298
Establishing a Compliance Assessment Team
  Enterprise Compliance, 133
Establishing an Effective GRC Culture
  Enterprise Objectives, 312
  Establishing of Enterprise-Wide Governance Awareness, 319
  Understanding the GRC Environment, 320
Establishing an Effective Risk Management Function
  Chief Risk Officer (CRO), 90
  Chief Risk Officer (CRO) Position Description, 93
  Continuous Risk Monitoring, 98
  CRO Responsibilities, 91
  Enterprise Risk Organization Responsibilities, 91
  Internal Audit, 94
Establishing of Enterprise-Wide Governance Awareness
  Communications to Stakeholders, 325
  Enterprise Codes of Conduct, 324
  Establishing an Effective GRC Culture, 319
  Ethics Attitude Surveys, 321
  Risk Management Course Outline, 327
Ethical Behavior and Integrity
  Enterprise Governance, 119
  SOx Mandates, 119

http://www.pbookshop.com

Ethical Business Practices
  Codes of Conduct, 122
Ethics Attitude Surveys
  Establishing of Enterprise-Wide Governance Awareness, 321
  Summarizing Ethics Survey Results, 323
Ethics Functions
  Enterprise Governance, 119
Event Identification
  COSO ERM Components, 66
  Significant Risk Events, 68
Event Inventories
  COSO ERM Guidance Material, 69
Example Company Background
  Global Computer Products Example Company, 17
Expected Value or Cost of Incurring a Risk
  Risk Response Planning, 44
Expected Values
  Quantitative Risk Analysis, 43
External Economic Events
  COSO ERM Components, 67

Facilitated Sessions
  Risk Monitoring, 86
Facilitated Workshops
  COSO ERM Guidance Material, 69
Facility Related-Risks
  Risk Transfer Processes, 106
Financial Officer Codes of Ethics or Conduct
  Sarbanes-Oxley Act (SOx), 197
Foreign Corrupt Practices Act (FCPA)
  Enterprise Governance Background, 118
Foreign Corrupt Practices Act of 1977
  COSO Internal Controls Background, 149

General Business Operations Risks
  Risk Transfer Processes, 105
Global Computer Products Example Company
  Corporate Risks Summary, 18
  Example Company Background, 17
  GRC Example Company, 16
Governance Principles
  GRC Concepts, 24
Governance, Risk and Compliance
  Enterprise Governance Practices, 15
  GRC Concepts, 15
Governance, Risk, and Compliance Principles
  Effective GRC Principles, 22
  GRC Concepts, 23
  GRC Governance Concepts, 24
Gramm-Leach-Bliley Act (GLBA)
  COSO ERM Control Activities, 95
GRC Attitude Survey Questions
  Understanding the GRC Environment, 322
GRC Best Practices
  Compliance-Related Requirements, 131
GRC Capability Context and Culture Elements
  OCEG Capability Model, 218
GRC Capability Organize and Oversee Elements
  OCEG Capability Model, 218
GRC Capability Prevent and Promote Elements
  OCEG Capability Model, 220
GRC Capability Processes
  OCEG Capability Model "Red Book," 215
  Open Compliance and Ethics Group (OCEG), 215
GRC Concepts
  Enterprise Compliance, 26
  Governance principles, 24
  Governance, Risk and Compliance, 15
  Governance, Risk, and Compliance Principles, 23
GRC Education Programs
  Building a GRC Culture, 326
GRC Example Company
  Global Computer Products Example Company, 16
GRC Governance Concepts
  Governance, Risk, and Compliance Principles, 24
  GRC Risk Management Processes, 25
GRC Practices
  Enterprise Governance Concepts, 116
GRC Principles
  Board of Directors Responsibilities, 228

http://www.pbookshop.com

- GRC Principles in the Board Room
  - Risk Committees, 240
- GRC Risk Management
  - COSO ERM, 25
- GRC Risk Management Processes
  - GRC Governance Concepts, 25

- Hotline Functions
  - Sarbanes-Oxley Act (SOx), 204
- Human Resource Standards
  - COSO ERM Components, 59
- Human Resources Policies and Practices
  - Control Environment Factors, 11
  - COSO Internal Controls Control Environment, 163

- IIA Risk Management Standards
  - COSO ERM, 250
  - International Standards for The Professional Practice of Internal Auditing, 249
- IIA standards
  - International Standards for The Professional Practice of Internal Auditing, 249
  - Risk-Based Internal Audit Standards, 249
- Implementing ERM
  - Risk Action Plans, 99
- Information and Communication
  - COSO ERM Components, 81
- Information and Communication Flows
  - COSO ERM Application Techniques, 82
  - COSO ERM Control Activities, 79
- Information Processing
  - COSO ERM Control Activities, 81
- Information Technology and Enterprise Risk Management
  - Application Development and Acquisition Risks, 295
  - Application Systems Risks, 292
  - Effective Continuity Planning, 292
  - Worms, Viruses, and System Network Risks, 307
  - Worms, Viruses, and Systems Network Access Risks, 292
- Inherent Risk
  - Risk Management Philosophy, 71
- In-House Developed Software
  - Application Systems Risks, 298
- Institute of Internal Auditors (IIA)
  - Internal Audit Responsibilities, 248
- Insurance Coverage
  - Risk Management Fundamentals, 32
  - Risk Transfer Processes, 107
- Integrating COSO ERM
  - COSO Internal Controls, 148
- Integrating Project Risk with Other Management Functions
  - Project management processes, 284
- Integrity and Ethical Values
  - Control Environment Factors, 6
  - COSO ERM Components, 57
  - COSO Internal Control Elements, 159
  - COSO Internal Control Environment Factors, 6
  - Tylenol Crisis, 57
- Internal Audit
  - Establishing an Effective Risk Management Function, 94
  - Risk Assessment Review and Internal Audit Report Comparison, 109
- Internal Audit Compliance Reviews
  - Effective Compliance Programs, 139
- Internal Audit Planning
  - COSO ERM, 251
- Internal Audit Plans
  - Risk Tolerance, 257
- Internal Audit Report Findings and Recommendations
  - Internal Audit Responsibilities, 264
- Internal Audit Responsibilities
  - Institute of Internal Auditors (IIA), 248
  - Internal Audit Report Findings and Recommendations, 264
  - Risk-Based Internal Audit Planning, 261
- Internal Control Evaluations
  - COSO Internal Control Monitoring, 172
  - Reporting Internal Control Deficiencies, 173
  - SOx Section 404, 182
- Internal Control–Integrated Framework
  - COSO Internal Controls Report, 3
- Internal Controls Background
  - COSO Internal Controls Framework, 2

http://www.pbookshop.com

- Internal Controls Definition
  - AICPA SAS No. 1, 148
  - AICPA SAS No. 55, 154
  - Separation of Duties Control, 1
  - Treadway Committee Report, 155
- Internal Environment
  - COSO ERM Components, 56
- Internal Infrastructure Events
  - COSO ERM Components, 68
- International Standards for The Professional Practice of Internal Auditing
  - IIA Risk Management Standards, 249
  - IIA standards, 249
- IT Business Outage Failure Impacts
  - IT Continuity Planning, 306
- IT Continuity Planning
  - Business Continuity Plans (BCPs), 304
  - IT Business Outage Failure Impacts, 306
  - IT Emergency Incident Response Plans, 304
  - IT General and Application Controls, 302
- IT Emergency Incident Response Plans
  - IT Continuity Planning, 304
- IT General and Application Controls
  - Business Continuity Plan Requirements, 305
  - COSO ERM, 293
  - Effective ERM Processes, 309
  - IT continuity Planning, 302
- IT General and Application-Specific Risks
  - Risk Transfer Processes, 106
- IT Internal Controls
  - System Balancing Procedures, 300

- Johnson & Johnson Credo
  - Tylenol crisis, 57

- Key Processes Identification
  - SOx Section 404 Internal Controls Assessments, 184
- Key Risk Assessments
  - Risk Identification, 37
- Knowledge Requirements
  - Risk Committees, 246

- Launching the Enterprise Help or Hotline Function
  - Whistleblower Programs, 207
- Legal and Regulatory Risks
  - Effective Enterprise Risk Management, 108
- Likelihood and Relative Significance Assessments
  - Enterprise Business Risks, 37
- Loss Event Data Tracking
  - COSO ERM Application Techniques, 70

- Management Compliance Reviews
  - Enterprise Compliance, 142
  - Enterprise GRC Programs, 144
- Management's Philosophy and Operating Style
  - Control Environment Factors, 9
  - COSO Internal Controls Control Environment, 161
- Minahan Committee
  - COSO Internal Controls Background, 154
- Mission Statements
  - COSO ERM Components, 62
  - Enterprise Governance Concepts, 120
- Modern Portfolio Theory
  - Risk Portfolio Management, 210
- Monitoring
  - COSO Internal Control Elements, 170
- Monte Carlo Risk Simulation Process Chart
  - Monte Carlo Simulation, 48
- Monte Carlo Simulation
  - Monte Carlo Risk Simulation Process Chart, 48
  - Quantitative Risk Analysis, 47

- National Commission on Fraudulent Financial Reporting
  - COSO Internal Controls Framework, 3
- National Commission on Fraudulent Reporting
  - Treadway Committee Report, 156
- National Institute of Science and Technology (NIST)
  - Enterprise Risk Management Guidance, 211

http://www.pbookshop.com

- Objective Setting
  - COSO ERM Components, 62
- OCEG Capability Model
  - Burgundy Book, 223
  - GRC Capability Context and Culture Elements, 218
  - GRC Capability Organize and Oversee Elements, 218
- OCEG Capability Model
  - GRC Capability Prevent and Promote Elements, 220
  - Principled Performance Concept, 217
  - Red Book, 215
- OCEG Capability Model “Red Book”
  - GRC Capability Processes, 215
- Officer Disclosure Sign-Offs
  - SOx Section 302, 196
- Open Compliance and Ethics Group (OCEG)
  - GRC Capability Processes, 215
- Organization Structure
  - Control Environment Factors, 10
- Organizing a Section 404 Internal Controls Review
  - Payroll Distribution Process Flowchart Example, 189
  - Section 404 Compliance Review Work Breakdown Structure, 186
  - SOx Section 404 Internal Controls Assessments, 184
- Payroll Distribution Process Flowchart Example
  - Organizing a Section 404 Internal Controls Review, 189
- PCAOB audit standards
  - SOx Section 404 Internal Controls Assessments, 193
- PCAOB Risk Standards
  - AS8 through AS15, 200
- Performance Indicators
  - COSO ERM Control Activities, 81
- PMBOK Guide
  - Project Risk Management Overview, 273
  - Risk Management Project Planning, 273
- Policies and Standards
  - Effective Enterprise Risk Management, 103
- Portfolio View of Risk
  - COSO ERM Framework, 51
  - COSO ERM Risk Assessment Process, 77
- Principal Agent Model
  - Enterprise Governance Concepts, 117
- Principled Performance Concept
  - OCEG Capability Model, 217
- Probability and Uncertainty
  - Risk Assessment Analysis, 39
- Process Flow Analysis
  - COSO ERM Guidance Material, 69
- Process Flowcharting
  - Risk Monitoring, 85
- Process Review Selection Guidelines
  - SOx Section 404 Internal Controls Assessments, 186
- Program Management Offices
  - Project Management Book of Knowledge (PMBOK), 289
- Project Life Cycles
  - Project Risk Management, 285
- Project Management Processes
  - Building a Project Management Organization, 288
  - Definition of Project Management, 267
  - Integrating Project Risk with Other Management Functions, 284
- Project Management Book of Knowledge (PMBOK)
  - Program Management Offices, 289
  - Project Management Institute (PMI), 269
  - Project Management Process, 270
  - Project Risk Management, 272
  - Risk Management Planning Inputs, 273
  - Risk Monitoring and Control, 282
  - Risk Response Planning, 279
- Project Management Decision Tree Analysis
  - Quantitative Risk Analysis, 280
- Project Management Institute (PMI)
  - Project Management Book of Knowledge (PMBOK), 269
- Project management knowledge areas
  - Project Management Planning, 271

http://www.pbookshop.com

- Project Management Planning
  - Project management knowledge areas, 271
- Project Management Process
  - Project Management Book of Knowledge (PMBOK), 270
- Project Planning
  - Risk Register Controls, 278
- Project Planning Risk Register Controls
  - Risk Identification, 277
- Project Risk Management
  - Project Life Cycles, 285
  - Project Management Book of Knowledge (PMBOK), 272
  - Risk Breakdown Structures, 275
  - Typical Project Risks, 286
- Project Risk Management Overview
  - PMBOK Guide, 273
- Promoting Enterprise Risk Concepts
  - Enterprise Objectives, 314
- Public Company Accounting Overview Board (PCAOB)
  - Sarbanes-Oxley Act (SOx), 179
- Purchased Software Contract Guidelines
  - Application Development and Acquisition Risks, 299

- Quality of Information
  - COSO Internal Controls Framework, 168
- Quantitative Risk Analysis
  - Decision Tree Analysis, 49
  - Delphi Method, 45
  - Expected Values, 43
  - Monte Carlo Simulation, 47
  - Project Management Decision Tree Analysis, 280
  - Response Planning, 43
  - Risk Management Project Planning, 279
  - Risk-Ranking Response-Planning, 44

- Ranking Internal Audit Risks
  - Auditable Entities, 260
- RAR Reports
  - Risk Assessment Reviews, 111
- RAR Sample Review Guidance
  - Risk Assessment Reviews (RARs), 110
- Red Book
  - OCEG Capability Model, 215
- Relative Risks versus Expected Returns
  - Defining the Risk Management Philosophy, 318
- Reporting Internal Control Deficiencies
  - Internal Control Evaluations, 173
- Residual Risk
  - Risk Management Philosophy, 71
- Response Planning
  - Quantitative Risk Analysis, 43
- Rights and Equitable Treatment of Shareholders
  - Enterprise Governance Concepts, 127
- Risk Acceptance
  - COSO ERM Components, 75
- Risk Action Plans
  - Continuous Risk Monitoring, 99
  - Implementing ERM, 99
- Risk Activity Scope
  - Effective Enterprise Risk Management, 97
- Risk Appetite
  - COSO ERM Components, 57
  - ERM Definitions and Objectives, 54
- Risk Appetite Map
  - COSO ERM Components, 61
- Risk Assessment
  - COSO ERM Components, 71
  - COSO Internal Control Elements, 13, 164
- Risk Assessment Acknowledgments
  - Risk Management Policies and Standards, 104
- Risk Assessment Analysis
  - Enterprise Business Risks, 38
  - Probability and Uncertainty, 39
  - Risk Interdependencies, 40
  - Risk Interdependency Hierarchy, 40
  - Risk Ranking, 41
- Risk Assessment as a Three-Step Process
  - COSO Internal Control Elements, 13
- Risk Assessment Matrix
  - Enterprise compliance, 138
- Risk Assessment Process
  - COSO ERM Control Activities, 79
  - COSO Internal Control Elements, 165
- Risk Assessment Review and Internal Audit Report Comparison
  - COSO ERM Control Activities, 109
  - Internal Audit, 109

http://www.pbookshop.com

Risk Assessment Reviews
  Board or Senior Management Risk Concerns, 112
  Effective Enterprise Risk Management, 111
  Enterprise Risk Awareness Programs, 112
  RAR Reports, 111
  Risk Awareness Newsletters, 113
  RAR Sample Review Guidance, 110
  Risk Management Policies and Standards, 109
Risk Avoidance
  COSO ERM Components, 74
Risk Awareness Guidelines
  Content Management, 101
Risk Awareness Newsletters
  Risk Assessment Reviews, 113
Risk Based Internal Audits
  COSO ERM, 248
Risk Breakdown Structures
  Project Risk Management, 275
Risk Committee Board Member Requirements
  Board of Directors Responsibilities, 242
  Risk Committees, 242
Risk Committees
  Board of Directors Responsibilities, 238
  GRC Principles in the Board Room, 240
  Knowledge Requirements, 246
  Risk Committee Board Member Requirements, 242
Risk Events
  Bhopal India, 42
  Dow Chemical Risk Event, 42
  Union Carbide Bhopal India Risk Event, 42
Risk Identification
  Brainstorming Approaches, 36
  Key Risk Assessments, 37
  Project Planning Risk Register Controls, 277
  Risk Management Fundamentals, 33
Risk Impact Matrix
  Risk Management Project Planning, 278
Risk Interdependencies
  Risk Assessment Analysis, 40
Risk Interdependency Hierarchy
  Risk Assessment Analysis, 40
Risk Likelihood and Impact Mapping
  COSO ERM Application Techniques, 70
  COSO ERM Risk Assessment Process, 74
Risk Management Corrective Action Practices
  Risk Management Policies and Standards, 109
Risk Management Course Outline
  Establishing of Enterprise-Wide Governance Awareness, 327
Risk Management Fundamentals
  Enterprise Business Risks, 35
  Enterprise Risk Model Framework, 34
  Insurance Coverage, 32
  Risk Identification, 33
  Risk Ranking, 41
Risk Management Organizations
  Effective Enterprise Risk Management, 101
Risk Management Philosophy
  COSO ERM Components, 56
  Inherent Risk, 71
  Residual Risk, 71
Risk Management Planning Inputs
  Project Management Book of Knowledge (PMBOK), 273
Risk Management Policies and Standards
  Effective Enterprise Risk Management, 100
Risk Management Policies and Standards
  Risk Assessment Acknowledgments, 104
  Risk Assessment Reviews (RARs), 109
  Risk Management Corrective Action Practices, 109
Risk Management Project Planning
  PMBOK Guide, 273
  Quantitative Risk Analysis, 279
  Risk Impact Matrix, 278
Risk Monitoring
  Benchmarking, 86
  Control Materials Reviews, 85
  COSO ERM Components, 84
  Dashboard Monitoring Tools, 66, 84
  Facilitated Sessions, 86
  Process Flowcharting, 85

http://www.pbookshop.com

Risk Monitoring and Control
  Project Management Book of Knowledge (PMBOK), 282
Risk Objective Setting Components
  COSO ERM Framework, 64
Risk Oversight Responsibilities
  Board of Directors Responsibilities, 233
Risk Portfolio Management
  Corporate Culture, 210
  Modern Portfolio Theory, 210
  Types of Risks Facing an Enterprise, 210
Risk Ranking
  Risk Assessment Analysis, 41
  Risk Management Fundamentals, 41
Risk Reduction
  COSO ERM Components, 75
Risk Register Controls
  Project Planning, 278
Risk Response Planning
  COSO ERM Guidance Material, 73
  Expected Value or Cost of Incurring a Risk, 44
  Project Management Book of Knowledge (PMBOK), 279
  Strategies for Dealing with Positive Risks, 281
Risk Sharing
  COSO ERM Components, 75
Risk Tolerance
  Internal Audit Plans, 257
Risk Transfer Processes
  IT General and Application-Specific Risks, 106
Risk Transfer Processes
  Facility Related-Risks, 106
  General Business Operations Risks, 105
  Insurance Coverage, 107
Risk-Awareness Cultures
  Effective Enterprise Risk Management, 100
Risk-Based Internal Audit Planning
  Internal Audit Responsibilities, 261
Risk-Based Internal Audit Standards
  IIA standards, 249
Risk-Ranking Response-Planning
  Quantitative Risk Analysis, 44
Roles and Responsibilities of the Board of Directors
  Enterprise Governance Concepts, 129

Sarbanes-Oxley Act (SOx)
  AS5 Risk-Based Auditing Standards, 198
  Board of Directors Responsibilities, 225
  COSO ERM, 177
  Enterprise Risk Management Concerns, 178
  Financial Officer Codes of Ethics or Conduct, 197
  Hotline Functions, 204
  Public Company Accounting Overview Board (PCAOB), 179
  Sarbanes-Oxley Act Key Provisions Summary, 181
  SOx Legislation Overview, 179
  Whistleblower Programs, 204
Sarbanes-Oxley Act Key Provisions Summary
  Sarbanes-Oxley Act (SOx), 181
SDLC Risks
  Application Development and Acquisition Risks, 297
SDLC Waterfall Model
  Application Development and Acquisition Risks, 296
SEC 1979 Internal Control Reporting Proposal
  COSO Internal Controls Background, 153
Section 404 Compliance Review Work Breakdown Structure
  Organizing a Section 404 Internal Controls Review, 186
Segregation of Duties
  COSO ERM Control Activities, 81
Selecting Key Processes for Review
  SOx Section 404 Internal Controls Assessments, 185
Separation of duties control
  Internal Controls Definition, 1
Significant Risk Events
  Event Identification, 68
SOx Legislation Overview
  Sarbanes-Oxley Act (SOx), 179

http://www.pbookshop.com

- SOxMandates
  - Ethical Behavior and Integrity, 119
- SOx Section 302
  - Corporate Responsibility for Financial Reports, 193
  - Officer Disclosure Sign-Offs, 196
- SOx Section 404
  - Internal Control Evaluations, 182
- SOx Section 404 Internal Controls Assessments
  - Accounts Payable Process Review Procedures, 191
  - Assessing Selected Process Risks, 190
  - Effectiveness of the Internal Control Structure Reports, 192
  - Enterprise Risk Management, 193
  - Key Processes Identification, 184
  - Organizing a Section 404 Internal Controls Review, 184
  - PCAOB Audit Standards, 193
  - Process Review Selection Guidelines, 186
  - Selecting Key Processes for Review, 185
- Strategic and Integrated Systems
  - COSO Internal Controls Framework, 167
- Strategies for Dealing with Positive Risks
  - Risk Response Planning, 281
- Summarizing Ethics Survey Results
  - Ethics Attitude Surveys, 323
- System Balancing Procedures
  - IT Internal Controls, 300
- System Development Life Cycle (SDLC)
  - Waterfall Development Processes, 295

- TreadwayCommission
  - COSO Internal Controls Background, 151
  - COSO Internal Controls Framework, 2
- Treadway Committee Report
  - Internal Controls Definition, 155
  - National Commission on Fraudulent Reporting, 156
- Tylenol crisis
  - Integrity and Ethical Values, 57
  - Johnson & Johnson Credo, 57
- Types of Risks Facing an Enterprise
  - Risk Portfolio Management, 210
- Typical Project Risks
  - Project Risk Management, 286
- U.S. Department of Labor Compliance-Related Laws
  - Enterprise Compliance, 140
- U.S. Federal Whistleblower Rules
  - Air 21 Statute, 205
  - Whistleblower Programs, 205

- Understanding the GRC Environment
  - Establishing an Effective GRC Culture, 320
  - GRC Attitude Survey Questions, 322
- Union Carbide Bhopal India Risk Event
  - Bhopal India, 42
  - Risk Events, 42

- Waterfall Development Processes
  - System Development Life Cycle (SDLC), 295
- Watergate Scandal
  - Enterprise Governance Background, 117
- Whistleblower Programs
  - Enterprise Compliance, 143
  - Launching the Enterprise Help or Hotline Function, 207
  - Sarbanes-Oxley Act (SOx), 204
  - U.S. Federal Whistleblower Rules, 205
- Work Unit–Level Compliance Tracking
  - Compliance Self-Audits, 141
  - Effective Compliance Programs, 139
- Worms, Viruses, and System Network Risks
  - Information Technology and Enterprise Risk Management, 307
- Worms, Viruses, and Systems Network Access Risks
  - Information Technology and Enterprise Risk Management, 292

http://www.pbookshop.com