

Contents

Preface xiii

PART I: IT GOVERNANCE CONCEPTS

Chapter 1: Importance of IT Governance for All Enterprises **3**

Chapter 2: Fundamental Governance Concepts and Sarbanes-Oxley Rules **9**

Sarbanes-Oxley Act 10

Other SOx Rules—Title II: Auditor Independence 18

SOx Title III: Corporate Responsibility 22

Title IV: Enhanced Financial Disclosures 24

What Is IT Governance? 28

Notes 35

Chapter 3: Enterprise Governance and GRC Tools **37**

The Road to Effective GRC Principles 38

Importance of GRC Governance 39

Risk Management Component of GRC 40

GRC and Enterprise Compliance 42

Importance of Effective GRC Practices and Principles 45

PART II: FRAMEWORKS TO SUPPORT EFFECTIVE IT GOVERNANCE

Chapter 4: IT Governance and COSO Internal Controls **49**

Importance of Effective Internal Controls and COSO 50

COSO Internal Control Systems Monitoring Guidance 65

Wrapping It Up: Importance of COSO Internal Controls	66
Notes	66
Chapter 5: COBIT and the IT Governance Institute	67
An Executive's Introduction to COBIT	68
The COBIT Framework and Its Drivers	70
COBIT Principle 1: Establish an Integrated IT Architecture Framework	72
COBIT Principle 2: Stakeholder Value Drivers	74
COBIT Principle 3: Focus on Business Context	75
COBIT Principle 4: Governance and Risk Management Enablers	78
COBIT Principle 5: Governance and Management Performance Measurement Structures	80
Putting It Together: Matching COBIT Processes and IT Goals	81
Using COBIT in a SOx Environment	84
COBIT in Perspective	85
Notes	86
Chapter 6: ITIL and IT Service Management Guidance	87
ITIL Fundamentals	88
ITIL Service Strategy Components	91
ITIL Service Design	94
ITIL Service Transition Management Processes	99
ITIL Service Operation Processes	102
IT Governance and ITIL Service Delivery Best Practices	106
Note	107
Chapter 7: IT Governance Standards: ISO 9001, 27002, and 38500	109
ISO Standards Background	110
ISO 9000 Quality Management Standards	112
ISO IT Security Standards: ISO 27002 and 27001	115
ISO 38500 IT Governance Standard	118
Notes	123
Chapter 8: IT Governance Issues: Risk Management, COSO ERM, and OCEG Guidance	125
Risk Management Fundamentals	126
COSO ERM Definitions and Objectives: A Portfolio View of Risk	134
COSO ERM Framework	136
Other Dimensions of the COSO ERM Framework	152
The OCEG GRC "Red Book," Risk Management, and IT Governance	153
Notes	157

PART III: TOOLS AND TECHNOLOGIES TO MANAGE THE IT GOVERNANCE INFRASTRUCTURE

Chapter 9: Cloud Computing, Virtualization, and Portable, Mobility Computing	161
Understanding Cloud Computing	162
IT Systems and Storage Management Virtualization	168
Smartphone and Handheld IT Device Governance Issues	175
Note	176
Chapter 10: Governance, IT Security, and Continuity Management	177
Importance of an Effective IT Security Environment	177
Enterprise IT Security Principles: Generally Accepted Security Standards	178
Importance of an Effective, Enterprise-Wide Security Strategy	185
IT Continuity Planning	186
The Business Continuity Plan and IT Governance	188
Notes	193
Chapter 11: PCI DSS Standards and Other IT Governance Rules	195
PCI DSS Background and Standards	196
Gramm-Leach-Bliley Act IT Governance Rules	203
HIPAA: Health Care and Much More	208
Notes	216
Chapter 12: IT Service Catalogs: Realizing Greater Value from IT Operations	217
Importance of IT Service Catalogs	219
Role of a Service Catalog in the IT Service Provider Organization	221
An IT Service Catalog's Content and Features	223
IT Service Catalog Management	224

PART IV: BUILDING AND MONITORING EFFECTIVE IT GOVERNANCE SYSTEMS

Chapter 13: Importance of IT Service-Oriented Architecture for IT Governance Systems	231
SOA Applications and Service-Driven IT Applications	232
SOA Governance, Internal Control Issues, and Risks	235
Planning and Building an SOA Implementation Blueprint	236
SOA and IT Governance	242
Notes	245

Chapter 14: IT Configuration and IT Portfolio Management	247
IT Configuration Management Concepts	248
ITIL Best Practices for IT Configuration Management	250
The Configuration Management Database: An Often Difficult Concept	254
Establishing an Enterprise CMDB	255
IT Portfolio Management	259
Chapter 15: Application Systems Implementations and IT Governance	263
The Systems Development Life Cycle: A Basic Application Development Technique	264
IT Rapid Development Processes: Prototyping	266
Enterprise Resource Planning and IT Governance Processes	268
Chapter 16: IT Governance Issues: Project and Program Management	275
The Project Management Process	275
PMBOK Standards	277
Another Project Management Standard: PRINCE2	280
IT Systems Portfolio and Program Management	280
The Program Management Office (PMO), a Strong Governance Resource	284
Project Management, the PMO, and IT Governance	286
Note	286
Chapter 17: Service Level Agreements, itSMF, Val IT, and Maximizing IT Investments	287
ITIL Service Management Best Practices and the itSMF	288
Open Compliance and Ethics Group (OCEG) Standards	292
Val IT: Enhancing the Value of IT Investments	298
Notes	305

PART V: MONITORING AND MEASURING ENTERPRISE MANAGEMENT AND BOARD GOVERNANCE

Chapter 18: Enterprise Content Management	309
ECM Characteristics and Key Components in the Enterprise Today	310
ECM Processes and IT Governance	310
Creating an Effective ECM Environment in the Enterprise	314

Chapter 19: Internal Audit's Governance Role	319
Internal Auditing History and Background	320
Internal Auditing and the IT Auditor	323
Internal Audit's IT Governance Activities and Responsibilities	323
Internal Audit IT Governance Standards	329
Internal Audit IT Governance Procedures	329
Note	334

PART VI: IT GOVERNANCE AND ENTERPRISE OBJECTIVES

Chapter 20: Creating and Sustaining an Ethical Workplace Culture	337
---	------------

Importance of Mission Statements	337
Enterprise Codes of Conduct	340
Whistleblower and Hotline Functions	347
Launching an Ethics Program and Improving Enterprise Governance Practices	352
Note	353

Chapter 21: Impact of Social Media Computing	355
---	------------

What Is Social Media Computing?	356
Social Media Examples	358
Enterprise Social Media Computing Risks and Vulnerabilities	365
Social Media Policies	367
Notes	370

Chapter 22: IT Governance and the Audit Committee's IT Role	371
--	------------

The Enterprise Audit Committee and IT Governance	371
Audit Committee IT Governance Responsibilities	374
Audit Committee Briefings and IT Governance Issues	375

About the Author 377

Index 379

<http://www.pbookshop.com>