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
Chapter 5: COBIT and the IT Governance Institute

An Executive’s Introduction to COBIT
The COBIT Framework and Its Drivers
COBIT Principle 1: Establish an Integrated IT Architecture Framework
COBIT Principle 2: Stakeholder Value Drivers
COBIT Principle 3: Focus on Business Context
COBIT Principle 4: Governance and Risk Management Enablers
COBIT Principle 5: Governance and Management Performance Measurement Structures
Putting It Together: Matching COBIT Processes and IT Goals
Using COBIT in a SOx Environment
COBIT in Perspective
Notes

Chapter 6: ITIL and IT Service Management Guidance

ITIL Fundamentals
ITIL Service Strategy Components
ITIL Service Design
ITIL Service Transition Management Processes
ITIL Service Operation Processes
IT Governance and ITIL Service Delivery Best Practices
Note

Chapter 7: IT Governance Standards: ISO 9001, 27002, and 38500

ISO Standards Background
ISO 9000 Quality Management Standards
ISO IT Security Standards: ISO 27002 and 27001
ISO 38500 IT Governance Standard
Notes

Chapter 8: IT Governance Issues: Risk Management, COSO ERM, and OCEG Guidance

Risk Management Fundamentals
COSO ERM Definitions and Objectives: A Portfolio View of Risk
COSO ERM Framework
Other Dimensions of the COSO ERM Framework
The OCEG GRC “Red Book,” Risk Management, and IT Governance
Notes
### PART III: TOOLS AND TECHNOLOGIES TO MANAGE THE IT GOVERNANCE INFRASTRUCTURE

**Chapter 9: Cloud Computing, Virtualization, and Portable, Mobility Computing**  
Understanding Cloud Computing  
IT Systems and Storage Management Virtualization  
Smartphone and Handheld IT Device Governance Issues  
Note

**Chapter 10: Governance, IT Security, and Continuity Management**  
Importance of an Effective IT Security Environment  
Enterprise IT Security Principles: Generally Accepted Security Standards  
Importance of an Effective, Enterprise-Wide Security Strategy  
IT Continuity Planning  
The Business Continuity Plan and IT Governance  
Notes

**Chapter 11: PCI DSS Standards and Other IT Governance Rules**  
PCI DSS Background and Standards  
Gramm-Leach-Bliley Act IT Governance Rules  
HIPAA: Health Care and Much More  
Notes

**Chapter 12: IT Service Catalogs: Realizing Greater Value from IT Operations**  
Importance of IT Service Catalogs  
Role of a Service Catalog in the IT Service Provider Organization  
An IT Service Catalog’s Content and Features  
IT Service Catalog Management

### PART IV: BUILDING AND MONITORING EFFECTIVE IT GOVERNANCE SYSTEMS

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