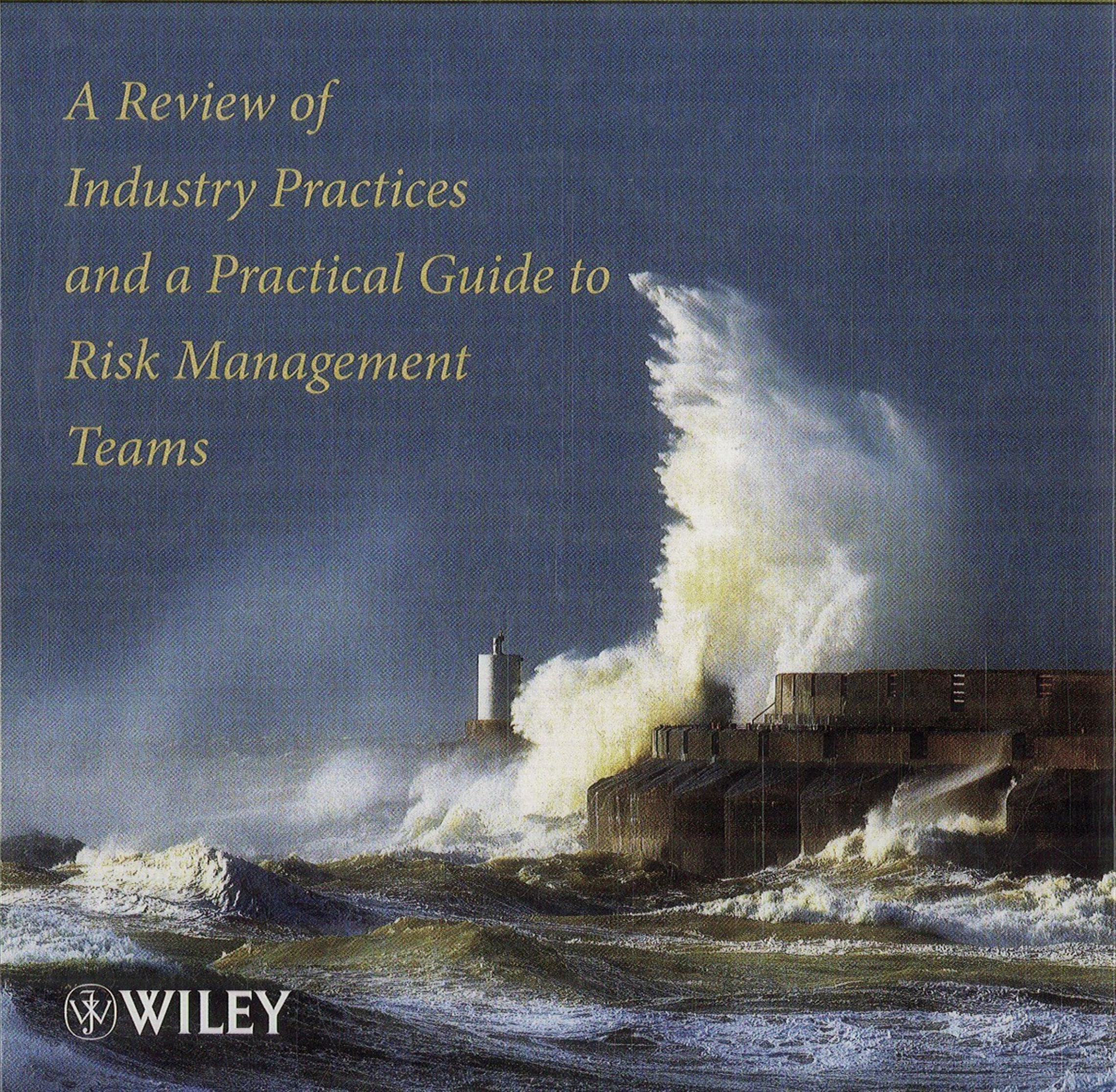
JAKE KOUNS AND DANIEL MINOLI

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

A Review of Industry Practices and a Practical Guide to Risk Management Teams



WILEY

CONTENTS

PREFACE xiii

ABOUT THE AUTHORS xv

PART I INDUSTRY PRACTICES IN RISK MANAGEMENT 1

1. INFORMATION SECURITY RISK MANAGEMENT IMPERATIVES AND OPPORTUNITIES 3

1.1 Risk Management Purpose and Scope 3

1.1.1 Purpose of Risk Management 3

1.1.2 Text Scope 17

References 24

Appendix 1A: Bibliography of Related Literature 25

2. INFORMATION SECURITY RISK MANAGEMENT DEFINED 33

2.1 Key Risk Management Definitions 33

2.1.1 Survey of Industry Definitions 33

2.1.2 Adopted Definitions 37

2.2 A Mathematical Formulation of Risk 40

2.2.1 What Is Risk? A Formal Definition 44

2.2.2 Risk in IT Environments 44

2.2.3 Risk Management Procedures 49

2.3 Typical Threats/Risk Events 56

2.4 What is an Enterprise Architecture? 61

References 65

Appendix 2A: The CISSPforum/ISO27k Implementers Forum Information Security Risk List for 2008 66

Appendix 2B: What is Enterprise Risk Management (ERM)? 71

3. INFORMATION SECURITY RISK MANAGEMENT STANDARDS 73

3.1 ISO/IEC 13335 77

3.2 ISO/IEC 17799 (ISO/IEC 27002:2005) 78

3.3 ISO/IEC 27000 SERIES 78

3.3.1 ISO/IEC 27000, Information Technology—Security Techniques—Information Security Management Systems—Fundamentals and Vocabulary 79
3.3.2 ISO/IEC 27001:2005, Information Technology—Security Techniques—Specification for an Information Security Management System 79
3.3.3 ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management 84
3.3.4 ISO/IEC 27003 Information Technology—Security Techniques—Information Security Management System Implementation Guidance 90
3.3.5 ISO/IEC 27004 Information Technology—Security Techniques—Information Security Management—Measurement 91
3.3.6 ISO/IEC 27005:2008 Information Technology—Security Techniques—Information Security Risk Management 92
3.4 ISO/IEC 31000 92
3.5 NIST STANDARDS 94
3.5.1 NIST SP 800-16 96
3.5.2 NIST SP 800-30 99
3.5.3 NIST SP 800-39 101
3.6 AS/NZS 4360 105
References 106
Appendix 3A: Organization for Economic CoOperation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security 107

4. A SURVEY OF AVAILABLE INFORMATION SECURITY RISK MANAGEMENT METHODS AND TOOLS 111

4.1 Overview 111
4.2 Risk Management/Risk Analysis Methods 114
4.2.1 Austrian IT Security Handbook 114
4.2.2 CCTA Risk Assessment and Management Methodology (CRAMM) 115
4.2.3 Dutch A&K Analysis 117
4.2.4 EBIOS 117
4.2.5 ETSI Threat Vulnerability and Risk Analysis (TVRA) Method 119
4.2.6 FAIR (Factor Analysis of Information Risk) 122
4.2.7 FIRM (Fundamental Information Risk Management) 124
4.2.8 FMEA (Failure Modes and Effects Analysis) 125

4.2.9 FRAP (Facilitated Risk Assessment Process) 128
4.2.10 ISAMM (Information Security Assessment and Monitoring Method) 129
4.2.11 ISO/IEC Baselines 130
4.2.12 ISO 31000 Methodology 130
4.2.13 IT-Grundschutz (IT Baseline Protection Manual) 136
4.2.14 MAGERIT (Metodologia de Analisis y Gestion de Riesgos de los Sistemas de Informacion) (Methodology for Information Systems Risk Analysis and Management) 137
4.2.15 MEHARI (Méthode Harmonisée d'Analyse de Risques—Harmonised Risk Analysis Method) 142
4.2.16 Microsoft's Security Risk Management Guide 146
4.2.17 MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale) 152
4.2.18 NIST 153
4.2.19 National Security Agency (NSA) IAM / IEM / IA-CMM 153
4.2.20 Open Source Approach 155
4.2.21 PTA (Practical Threat Analysis) 158
4.2.22 SOMAP (Security Officers Management and Analysis Project) 160
4.2.23 Summary 161
References 162

5. **METHODOLOGIES EXAMPLES: COBIT AND OCTAVE 164**

5.1 Overview 164
5.2 COBIT 166
5.2.1 COBIT Framework 172
5.2.2 The Need for a Control Framework for IT Governance 173
5.2.3 How COBIT Meets the Need 175
5.2.4 COBIT's Information Criteria 175
5.2.5 Business Goals and IT Goals 176
5.2.6 COBIT Framework 177
5.2.7 IT Resources 178
5.2.8 Plan and Organize (PO) 180
5.2.9 Acquire and Implement (AI) 180
5.2.10 Deliver and Support (DS) 180
5.2.11 Monitor and Evaluate (ME) 181
5.2.12 Processes Need Controls 181
5.2.13 COBIT Framework 181
5.2.14 Business and IT Controls 184
5.2.15 IT General Controls and Application Controls 185

5.2.16 Maturity Models 187
5.2.17 Performance Measurement 194
5.3 OCTAVE 205
5.3.1 The OCTAVE Approach 205
5.3.2 The OCTAVE Method 208
References 210

PART II DEVELOPING RISK MANAGEMENT TEAMS 211

6. RISK MANAGEMENT ISSUES AND ORGANIZATION SPECIFICS 213

6.1 Purpose and Scope 213
6.2 Risk Management Policies 216
6.3 A Snapshot of Risk Management in the Corporate World 219
6.3.1 Motivations for Risk Management 224
6.3.2 Justifying Risk Management Financially 225
6.3.3 The Human Factors 230
6.3.4 Priority-Oriented Rational Approach 232
6.4 Overview of Pragmatic Risk Management Process 234
6.4.1 Creation of a Risk Management Team, and Adoption of Methodologies 234
6.4.2 Iterative Procedure for Ongoing Risk Management 236
6.5 Roadmap to Pragmatic Risk Management 236
References 239
Appendix 6A: Example of a Security Policy 239

7. ASSESSING ORGANIZATION AND ESTABLISHING RISK MANAGEMENT SCOPE 243

7.1 Assessing the Current Enterprise Environment 244
7.2 Soliciting Support From Senior Management 248
7.3 Establishing Risk Management Scope and Boundaries 259
7.4 Defining Acceptable Risk for Enterprise 260
7.5 Risk Management Committee 263
7.6 Organization-Specific Risk Methodology 264
7.6.1 Quantitative Methods 265
7.6.2 Qualitative Methods 267
7.6.3 Other Approaches 269
7.7 Risk Waivers Programs 272
References 274
Appendix 7A: Summary of Applicable Legislation 275

8. IDENTIFYING RESOURCES AND IMPLEMENTING THE RISK MANAGEMENT TEAM 280

8.1 Operating Costs to Support Risk Management and Staffing Requirements 281
8.2 Organizational Models 286
8.3 Staffing Requirements 287
8.3.1 Specialized Skills Required 290
8.3.2 Sourcing Options 291
8.4 Risk Management Tools 295
8.5 Risk Management Services 296
8.5.1 Alerting and Analysis Services 296
8.5.2 Assessments, Audits, and Project Consulting 296
8.6 Developing and Implementing the Risk Management/ Assessment Team 298
8.6.1 Creating Security Standards 298
8.6.2 Defining Subject Matter Experts 300
8.6.3 Determining Information Sources 300
References 301
Appendix 8A: Sizing Example for Risk Management Team 302
Appendix 8B: Example of Vulnerability Alerts by Vendors and CERT 331
Appendix 8C: Examples of Data Losses—A One-Month Snapshot 336

9. IDENTIFYING ASSETS AND ORGANIZATION RISK EXPOSURES 338

9.1 Importance of Asset Identification and Management 338
9.2 Enterprise Architecture 340
9.3 Identifying IT Assets 346
9.4 Assigning Value to IT Assets 353
9.5 Vulnerability Identification/Classification 354
9.5.1 Base Parameters 360
9.5.2 Temporal Parameters 362
9.5.3 Environmental Parameters 363
9.6 Threat Analysis: Type of Risk Exposures 367
9.6.1 Type of Risk Exposures 368
9.6.2 Internal Team Programs (to Uncover Risk Exposures) 371
9.7 Summary 371
References 371
Appendix 9A: Common Information Systems Assets 372

10. REMEDIATION PLANNING AND COMPLIANCE REPORTING 377

10.1 Determining Risk Value 377
10.2 Remediation Approaches 380

10.3 Prioritizing Remediations 384
10.4 Determining Mitigating Timeframes 385
10.5 Compliance Monitoring and Security Metrics 387
10.6 Compliance Reporting 390
References 391

BASIC GLOSSARY OF TERMS USED IN THIS TEXT 392

***INDEX* 415**