Contents

CONTENTS IV

FIGURES VIII

TABLES X

ABOUT THE EXAM 11

HOW TO USE THIS BOOK 12

SECTION 1: THE BASICS 14

CHAPTER 1: SECURITY CONCEPTS 15

CHAPTER 2: GOVERNANCE, GOALS, STRATEGIES, POLICIES, STANDARDS AND PROCEDURES 17

CHAPTER 3: STRATEGY 23

CHAPTER 4: RISK APPETITE, TOLERANCE AND CAPACITY 27

CHAPTER 5: ANALYSIS OF RISK 31

CHAPTER 6: CONTROLLING THREATS AND RISK 36

CHAPTER 7: CONTROLS AND COUNTERMEASURES 47

CHAPTER 8: ALE, RTO, RPO, SDO, MTO, MTD AND AIW 59

CHAPTER 9: BCP, DRP AND BIA 64

CHAPTER 10: BUSINESS CONTINUITY AND DISASTER RECOVERY 67

CHAPTER 11: TESTING INCIDENT RESPONSE, BUSINESS CONTINUITY PLANS AND DISASTER RECOVERY PLANS 78

CHAPTER 12: ROLES, RESPONSIBILITIES, RACI AND SKILLS 81

CHAPTER 13: DUE DILIGENCE AND DUE CARE 83

CHAPTER 14: SECURITY PRINCIPLES 85

CHAPTER 15: KGIS, KPIS, KRIS AND CSFS 87

CHAPTER 16: TECHNOLOGIES 88

CHAPTER 17: STANDARDS AND FRAMEWORKS 90

CHAPTER 18: CULTURE 100

CHAPTER 19: METRICS 102

CHAPTER 20: CURRENT STATE, DESIRED STATE AND THE GAP IN-BETWEEN 103

CHAPTER 21: INFORMATION SECURITY INFRASTRUCTURE AND ARCHITECTURE 106

CHAPTER 22: CLOUD COMPUTING 109

CHAPTER 23: METRICS DEVELOPMENT 116

CHAPTER 24: BUSINESS MODEL FOR INFORMATION SECURITY (BMIS) 118

SECTION 2: THE FOUR DOMAINS 123

CHAPTER 25: INFORMATION SECURITY GOVERNANCE – OVERVIEW 125

CHAPTER 26: INFORMATION SECURITY GOVERNANCE – THE GOAL 128

CHAPTER 27: INFORMATION SECURITY GOVERNANCE – THE STRATEGY 130

CHAPTER 28: INFORMATION SECURITY GOVERNANCE – WHO DOES WHAT 134

CHAPTER 29: INFORMATION SECURITY GOVERNANCE – RESOURCES THAT HELP 140

CHAPTER 30: INFORMATION SECURITY GOVERNANCE – CONSTRAINTS THAT HURT 154

CHAPTER 31: INFORMATION SECURITY GOVERNANCE – THE ACTION PLAN 158

CHAPTER 32: INFORMATION SECURITY GOVERNANCE – METRICS AND MONITORING 162

CHAPTER 33: INFORMATION SECURITY GOVERNANCE – WHAT SUCCESS LOOKS LIKE 170

CHAPTER 34: INFORMATION RISK MANAGEMENT – OVERVIEW 172

CHAPTER 35: INFORMATION RISK MANAGEMENT – THE GOAL 189

CHAPTER 36: INFORMATION RISK MANAGEMENT – THE STRATEGY 192

CHAPTER 37: INFORMATION RISK MANAGEMENT – WHO DOES WHAT 194

CHAPTER 38: INFORMATION RISK MANAGEMENT – RESOURCES THAT HELP 200

CHAPTER 39: INFORMATION RISK MANAGEMENT – CONSTRAINTS THAT HURT 214

CHAPTER 40: INFORMATION RISK MANAGEMENT – THE ACTION PLAN 219

CHAPTER 41: INFORMATION RISK MANAGEMENT – METRICS, MONITORING AND REPORTING 245

CHAPTER 42: INFORMATION RISK MANAGEMENT – WHAT SUCCESS LOOKS LIKE 250

CHAPTER 43: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – OVERVIEW 251

CHAPTER 44: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – THE GOAL .252

CHAPTER 45: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – THE STRATEGY 253

CHAPTER 46: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – WHO DOES WHAT 255

CHAPTER 47: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – RESOURCES THAT HELP 256

CHAPTER 48: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – CONSTRAINTS THAT HURT 257

CHAPTER 49: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – THE ACTION PLAN 261

CHAPTER 50: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – METRICS AND MONITORING 264

CHAPTER 51: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT – WHAT SUCCESS LOOKS LIKE 271

CHAPTER 52: INFORMATION SECURITY INCIDENT MANAGEMENT – OVERVIEW 274

CHAPTER 53: INFORMATION SECURITY INCIDENT MANAGEMENT – THE GOAL...................................277

CHAPTER 54: INFORMATION SECURITY INCIDENT MANAGEMENT – THE STRATEGY 279

CHAPTER 55: INFORMATION SECURITY INCIDENT MANAGEMENT – WHO DOES WHAT.......................280

CHAPTER 56: INFORMATION SECURITY INCIDENT MANAGEMENT – RESOURCES THAT HELP 287

CHAPTER 57: INFORMATION SECURITY INCIDENT MANAGEMENT – CONSTRAINTS THAT HURT 289

CHAPTER 58: INFORMATION SECURITY INCIDENT MANAGEMENT – THE ACTION PLAN 290

CHAPTER 59: INFORMATION SECURITY INCIDENT MANAGEMENT – METRICS AND MONITORING 291

CHAPTER 60: INFORMATION SECURITY INCIDENT MANAGEMENT – WHAT SUCCESS LOOKS LIKE 292

ACRONYMS 293

DEFINITIONS **298**

INDEX **334**

Figures

Figure 1: Goals, Strategies, Policies, Standards, Procedures and Guidelines 17
Figure 2: Optimizing Risk Costs 28
Figure 3: Qualitative Impact Matrix 32
Figure 4: Semiquantitative Matrix 33
Figure 5: Information Security Relationships 36
Figure 6: Control Types and Effect 49
Figure 7:Techniques Implemented in Relation to RTOs and RPOs 75
Figure 8: COBIT 5 Principles 91
Figure 9: COBIT 5 Enterprise Enablers 93
Figure 10: Overview of the Process Assessment Model 94
Figure 11: TOGAF Architecture Development Cycle 96
Figure 12: Characteristics of CMMI Maturity Levels 97
Figure 13: Balanced Scorecard Dimensions 98
Figure 14: How Cultures are Created 101
Figure 15: Common Framework Layers 108
Figure 16: Enterprise Architecture Domains 107
Figure 17: Classic Architecture vs. Cloud Computing 109
Figure 18: Cloud Computing Deployment Models 110
Figure 19: 'as a Service' Offerings 111
Figure 20: Cloud Computing Risk Map 114
Figure 21: Business Model for Information Security 118
Figure 22: Governance Relationships 126
Figure 23: Information Security Strategy Development Participants 130
Figure 24: Prevalent Standards and Frameworks 133
Figure 25: Relationship of Governance Elements 159
Figure 26: Components of Security Metrics 165
Figure 27: The IT Risk Management Life Cycle 176
Figure 28: Top Layer of Business Risk Structure 201
Figure 29: Critical Function Layer of Business Risk Structure 201
Figure 30: Aligning Assets to the Critical Layer Function 202
Figure 31: Asset Vulnerabilities 202
Figure 32: Combined Impact Risk Structure 203
Figure 33: Risk Analysis Framework 204

Figure 34: Factor analysis of information risk (FAIR) 207
Figure 35: Risk Scenario Structure 211
Figure 36: PDCA Methodology.. 212
Figure 37: Strategic Goals, CSFs, KPIs and Key Actions.. 213
Figure 38: Disconnect of Responsibilities with Outsourced Providers 214
Figure 39: Continuous Risk Management Steps 225
Figure 40: Steps to Information Security Program Development 254
Figure 41: Incident Response Plan Process Flow 261
Figure 42: Incident Management Life Cycle Phases 278

Tables

Table 1: Basic Recovery Tests and Categories ... 79
Table 2: A RACI Example ... 82
Table 3: Roles and Responsibilities RACI Matrix ... 138
Table 4: Security Content and Application ... 222
Table 5: Security Incident Roles and Responsibilities ... 283

About the Exam

The CISM, or Certified Information Security Manager Certification, is one of the most recognized credentials for information security managers and has been awarded to more than 27,000 professionals to-date.

Beyond passing the exam, a CISM Certification requires a minimum of five years of experience in information security, and a minimum of two years of experience as an information security manager. If you have a CISA or CISSP certification, or a post-graduate degree in information security or other related field, then you are eligible to substitute two years of work experience. Finally, you will be required to and agree and comply with the ISACA's Code of Professional Ethics and the CISM Continuing Education Policy.

The exam cost between $625 and $750. If you pay to register as a member with ISACA, you can receive a discount. ISACA offers a free self-assessment exam with 50 questions to test your readiness for the actual exam. You can register for the CISM exam on the ISACA website. The day of the test you must bring a photo ID and the admissions ticket provided after you register.

The CISM exam is given twice per year in June and December. The test will take four hours and includes 200 total questions, giving you just over one minute per question. You are awarded 4 points per each correctly answered question, and a minimum score of 450, or roughly 113 correct questions, is required to pass the test.

Once you pass the test and have the score in-hand, you can submit your CISM application to get your certification. This requires proof of five years of experience of work, with signed verification from your employers.

There is only a 50-60% first time pass rate, so study the material repeatedly and take multiple assessment tests prior to taking the plunge.