
Contents

Biography xix

1 Introduction 1

1.1 The Role of the Information Security Manager 1

1.1.1 Audit as a Driver for Security Initiatives 2

1.1.2 Technology as a Driver for Security Initiatives 2

1.1.3 Compliance as a Driver for Security Initiatives 2

1.1.4 Security Risk as a Driver for Security Initiatives 2

1.2 Ensuring a Quality Information Security Risk Assessment 3

1.3 Security Risk Assessment 3

1.3.1 The Role of the Security Risk Assessment 4

1.3.2 Definition of a Security Risk Assessment 5

1.3.3 The Need for a Security Risk Assessment 7

1.3.3.1 Checks and Balances 7

1.3.3.2 Periodic Review 7

1.3.3.3 Risk-Based Spending 8

1.3.3.4 Requirement 10

1.3.4 Security Risk Assessment Secondary Benefits 10

1.4 Related Activities 11

1.4.1 Gap Assessment 11

1.4.2 Compliance Audit 13

1.4.3 Security Audit 14

1.4.4 Vulnerability Scanning 14

1.4.5 Penetration Testing 15

1.4.6 Ad Hoc Testing 15

1.4.7 Social Engineering 15

1.4.8 War Dialing 15

1.5 The Need for This Book 16

1.6 Who Is This Book For? 18

Exercises 19

Notes 20

References.....	21
Bibliography	21
2 Information Security Risk Assessment Basics.....	23
2.1 Phase 1: Project Definition	23
2.2 Phase 2: Project Preparation	25
2.3 Phase 3: Data Gathering.....	25
2.4 Phase 4: Risk Analysis	25
2.4.1 Assets.....	26
2.4.2 Threat Agents and Threats	27
2.4.2.1 Threat Agents	27
2.4.2.2 Threats.....	28
2.4.3 Vulnerabilities.....	29
2.4.4 Security Risk	30
2.5 Phase 5: Risk Mitigation	31
2.5.1 Safeguards	31
2.5.2 Residual Security Risk.....	33
2.6 Phase 6: Risk Reporting and Resolution.....	33
2.6.1 Risk Resolution	34
Exercises.....	35
Notes	36
References.....	37
3 Project Definition.....	39
3.1 Ensuring Project Success	39
3.1.1 Success Definition	40
3.1.1.1 Customer Satisfaction.....	40
3.1.1.2 Quality of Work	44
3.1.1.3 Completion within Budget.....	49
3.1.2 Setting the Budget.....	50
3.1.3 Determining the Objective.....	51
3.1.4 Limiting the Scope	52
3.1.4.1 Underscoping	52
3.1.4.2 Overscoping	53
3.1.4.3 Security Controls.....	54
3.1.4.4 Assets.....	55
3.1.4.5 Reasonableness in Limiting the Scope	56
3.1.5 Identifying System Boundaries.....	56
3.1.5.1 Physical Boundary	57
3.1.5.2 Logical Boundaries.....	58
3.1.6 Specifying the Rigor	60
3.1.7 Sample Scope Statements.....	60

3.2	Project Description.....	62
3.2.1	Project Variables	62
3.2.2	Statement of Work.....	63
3.2.2.1	Specifying the Service Description	63
3.2.2.2	Scope of Security Controls	63
3.2.2.3	Specifying Deliverables.....	64
3.2.2.4	Contract Type	66
3.2.2.5	Contract Terms	67
	Exercises.....	70
	Notes	71
	References.....	72
4	Security Risk Assessment Preparation	73
4.1	Introduce the Team	73
4.1.1	Introductory Letter.....	74
4.1.2	Pre-Assessment Briefing.....	74
4.1.3	Obtain Proper Permission.....	75
4.1.3.1	Policies Required	76
4.1.3.2	Permission Required.....	76
4.1.3.3	Scope of Permission	77
4.1.3.4	Accounts Required	78
4.2	Review Business Mission	78
4.2.1	What Is a Business Mission?	79
4.2.2	Obtaining Business Mission Information	80
4.3	Identify Critical Systems.....	81
4.3.1	Determining Criticality.....	81
4.3.1.1	Approach 1: Find the Information Elsewhere	83
4.3.1.2	Approach 2: Create the Information on a High Level.....	83
4.3.1.3	Approach 3: Classify Critical Systems.....	83
4.4	Identify Assets	85
4.4.1	Checklists and Judgment	86
4.4.2	Asset Sensitivity/Criticality Classification.....	86
4.4.2.1	Approach 1: Find Asset Classification Information Elsewhere.....	86
4.4.2.2	Approach 2: Create Asset Classification Information	86
4.4.2.3	Approach 3: Determine Asset Criticality	89
4.4.3	Asset Valuation	91
4.4.3.1	Approach 1: Binary Asset Valuation	91
4.4.3.2	Approach 2: Classification-Based Asset Valuation	91

4.4.3.3	Approach 3: Rank-Based Asset Valuation	92
4.4.3.4	Approach 4: Consensus Asset Valuation	93
4.4.3.5	Approaches 5–7: Accounting Valuation Approaches	93
4.5	Identifying Threats	95
4.5.1	Threat Components	96
4.5.1.1	Threat Agent	96
4.5.1.2	Undesirable Events	96
4.5.2	Listing Possible Threats	96
4.5.2.1	Checklists and Judgment	99
4.5.2.2	Threat Agent and Undesirable Event Pairing	99
4.5.3	Threat Statements	101
4.5.4	Validating Threat Statements	102
4.5.4.1	Factors Affecting Threat Statement Validity	102
4.6	Determine Expected Controls	104
	Exercises	108
	Notes	108
	References	110
	Bibliography	110
5	Data Gathering	111
5.1	Sampling	112
5.1.1	Sampling Objectives	114
5.1.2	Sampling Types	115
5.1.3	Use of Sampling in Security Testing	116
5.1.3.1	Approach 1: Representative Testing	116
5.1.3.2	Approach 2: Selected Sampling	116
5.1.3.3	Approach 3: Random Sampling	117
5.2	The RIIOT Method of Data Gathering	117
5.2.1	RIIOT Method Benefits	118
5.2.2	RIIOT Method Approaches	118
5.2.2.1	Review Documents or Designs	119
5.2.2.2	Interview Key Personnel	125
5.2.2.3	Inspect Security Controls	132
5.2.2.4	Observe Personnel Behavior	134
5.2.2.5	Test Security Controls	136
5.2.3	Using the RIIOT Method	140
	Exercises	141
	Notes	141
	References	143
6	Administrative Data Gathering	145
6.1	Threats and Safeguards	145

6.1.1	Human Resources	146
6.1.1.1	Recruitment.....	146
6.1.1.2	Employment.....	151
6.1.1.3	Termination.....	154
6.1.2	Organizational Structure.....	154
6.1.2.1	Senior Management.....	155
6.1.2.2	Security Program.....	156
6.1.2.3	Security Operations.....	156
6.1.2.4	Audit	157
6.1.3	Information Control.....	158
6.1.3.1	User Accounts.....	158
6.1.3.2	User Error.....	159
6.1.3.3	Asset Control.....	160
6.1.3.4	Sensitive Information.....	160
6.1.4	Business Continuity.....	161
6.1.4.1	Contingency Planning.....	162
6.1.4.2	Incident Response Program	163
6.1.5	System Security	163
6.1.5.1	System Controls.....	163
6.1.5.2	Application Security	165
6.1.5.3	Configuration Management	166
6.1.5.4	Third-Party Access.....	166
6.2	The RIOT Method: Administrative Data Gathering	167
6.2.1	Review Administrative Documents	173
6.2.1.1	Documents to Request	173
6.2.1.2	Review Documents for Clarity, Consistency, and Completeness	173
6.2.1.3	Reviewing Documents Other than Policies	177
6.2.2	Interview Administrative Personnel.....	186
6.2.2.1	Administrative Interview Topics.....	186
6.2.2.2	Administrative Interview Subjects	187
6.2.2.3	Administrative Interview Questions	188
6.2.3	Inspect Administrative Security Controls.....	192
6.2.3.1	Listing Administrative Security Controls.....	192
6.2.3.2	Verify Information Gathered.....	192
6.2.3.3	Determine Vulnerabilities.....	194
6.2.3.4	Document and Review Findings	194
6.2.3.5	Inspect the Security Organization	194
6.2.4	Observe Administrative Behavior	199
6.2.5	Test Administrative Security Controls.....	200
6.2.5.1	Information Labeling Testing.....	200

6.2.5.2	Media Destruction Testing.....	200
6.2.5.3	Account and Access Control Procedures Testing.....	207
6.2.5.4	Outsourcing and Information Exchange	209
	Exercises.....	211
	Notes	212
	References.....	214
	Bibliography	214
7	Technical Data Gathering.....	215
7.1	Technical Threats and Safeguards.....	215
7.1.1	Information Control.....	215
7.1.1.1	User Error.....	215
7.1.1.2	Sensitive and Critical Information.....	219
7.1.1.3	User Accounts.....	219
7.1.2	Business Continuity.....	220
7.1.2.1	Contingency Planning.....	221
7.1.3	System Security	221
7.1.3.1	System Controls.....	221
7.1.3.2	Application Security	222
7.1.3.3	Change Management	223
7.1.4	Secure Architecture	223
7.1.4.1	Topology	224
7.1.4.2	Transmission	225
7.1.4.3	Perimeter Network	226
7.1.5	Components	227
7.1.5.1	Access Control.....	227
7.1.5.2	Intrusion Detection	228
7.1.6	Configuration.....	229
7.1.6.1	System Settings.....	229
7.1.7	Data Security.....	230
7.1.7.1	Storage.....	230
7.1.7.2	Transit	230
7.2	The RIIOT Method: Technical Data Gathering.....	231
7.2.1	Review Technical Documents	231
7.2.1.1	Technical Documents to Request	231
7.2.1.2	Review Technical Documents for Information	231
7.2.1.3	Review Technical Security Designs	236
7.2.2	Interview Technical Personnel	248
7.2.2.1	Technical Interview Topics.....	248
7.2.2.2	Technical Interview Subjects	248
7.2.2.3	Technical Interview Questions	248

7.2.3	Inspect Technical Security Controls	249
7.2.3.1	List Technical Security Controls.....	251
7.2.3.2	Verify Information Gathered	255
7.2.3.3	Determine Vulnerabilities.....	262
7.2.3.4	Document and Review Findings	262
7.2.4	Observe Technical Personnel Behavior	262
7.2.5	Test Technical Security Controls	265
7.2.5.1	Monitoring Technology.....	265
7.2.5.2	Audit Logs.....	266
7.2.5.3	Anti-Virus Systems	266
7.2.5.4	Automated Password Policies.....	267
7.2.5.5	Virtual Private Network	267
7.2.5.6	Firewalls, IDS, and System Hardening.....	268
7.2.5.7	Vulnerability Scanning.....	268
7.2.5.8	Penetration Testing.....	279
7.2.5.9	Testing Specific Technology	280
	Exercises	283
	Notes	283
	Reference	285
	Bibliography	285
8	Physical Data Gathering	287
8.1	Physical Threats and Safeguards	288
8.1.1	Utilities and Interior Climate	288
8.1.1.1	Power.....	288
8.1.1.2	Heat.....	292
8.1.1.3	Humidity	293
8.1.2	Fire	293
8.1.2.1	Fire Impact and Likelihood	295
8.1.2.2	Fire Safeguards	295
8.1.2.3	Fire Alarm Systems.....	296
8.1.2.4	Fire Alarm Installation Types	301
8.1.2.5	Fire Suppression.....	303
8.1.2.6	Fire Evacuation.....	305
8.1.3	Flood and Water Damage.....	306
8.1.4	Lightning.....	308
8.1.5	Earthquakes.....	309
8.1.6	Volcanoes.....	310
8.1.7	Landslides.....	310
8.1.8	Hurricanes.....	310
8.1.9	Tornadoes.....	312
8.1.10	Natural Hazards Summary.....	312
8.1.11	Human Threats to Physical Security.....	312

- 8.1.11.1 Personnel Screening..... 314
 - 8.1.11.2 Barriers..... 315
 - 8.1.11.3 Lighting..... 316
 - 8.1.11.4 Intrusion Detection 317
 - 8.1.11.5 Physical Access Control 321
 - 8.1.11.6 Preventing Unauthorized Entry 321
 - 8.1.11.7 Preventing Unauthorized Removal 325
 - 8.2 The RIIOT Method: Physical Data Gathering 325
 - 8.2.1 Review Physical Documents..... 325
 - 8.2.1.1 Physical Documents to Request..... 328
 - 8.2.1.2 Review Physical Documents for Information ... 328
 - 8.2.2 Interview Physical Personnel..... 337
 - 8.2.2.1 Physical Security Interview Topics..... 337
 - 8.2.2.2 Physical Security Interview Subjects 337
 - 8.2.2.3 Physical Security Interview Questions 338
 - 8.2.3 Inspect Physical Security Controls..... 338
 - 8.2.3.1 Listing Physical Security Controls 338
 - 8.2.3.2 Verify Information Gathered 341
 - 8.2.3.3 Determine Physical Vulnerabilities 348
 - 8.2.3.4 Document and Review Physical Findings..... 348
 - 8.2.4 Observe Physical Personnel Behavior..... 348
 - 8.2.5 Test Physical Security Safeguards 352
 - 8.2.5.1 Doors and Locks 352
 - 8.2.5.2 Intrusion Detection 352
 - Exercises..... 352
 - Notes 362
 - References..... 363
 - 9 Security Risk Analysis..... 365**
 - 9.1 Determining Security Risk..... 365
 - 9.1.1 Uncertainty and Reducing Uncertainty..... 366
 - 9.1.1.1 Review Available Data 369
 - 9.1.1.2 Examine Historical Data 369
 - 9.1.1.3 Use Judgment 369
 - 9.1.1.4 Use Tools..... 371
 - 9.1.1.5 Use Conditional Probabilities 371
 - 9.2 Creating Security Risk Statements..... 374
 - 9.3 Team Review of Security Risk Statements 375
 - 9.3.1 Obtaining Consensus 375
 - 9.3.2 Deriving Overall Security Risk..... 378
 - Exercises..... 378
 - Notes 378
 - References..... 379

10 Security Risk Mitigation	381
10.1 Selecting Safeguards	381
10.1.1 Method 1: Missing Control Leads to Implementing Safeguard.....	382
10.1.2 Method 2: People, Process, Technology	382
10.1.3 Method 3: Administrative, Physical, Technical	382
10.1.4 Method 4: Preventive, Detective, Corrective	382
10.1.5 Method 5: Available Technology	383
10.2 Safeguard Solution Sets	383
10.2.1 Safeguard Cost Calculations.....	385
10.2.2 Justifying Safeguard Selections.....	386
10.2.2.1 Justification through Judgment	386
10.2.2.2 Cost–Benefit Analysis.....	387
10.3 Establishing Security Risk Parameters.....	389
Exercises	392
Notes	392
Bibliography	393
11 Security Risk Assessment Reporting.....	395
11.1 Cautions in Reporting.....	395
11.2 Pointers in Reporting.....	397
11.3 Report Structure.....	397
11.3.1 Executive-Level Report.....	398
11.3.2 Base Report	398
11.3.3 Appendices and Exhibits	399
11.4 Document Review Methodology: Create the Report Using a Top-Down Approach.....	400
11.4.1 Document Specification	401
11.4.2 Draft	404
11.4.3 Final.....	405
11.5 Assessment Brief.....	405
11.6 Action Plan.....	406
Exercises	406
Note.....	407
References.....	407
Bibliography	407
12 Security Risk Assessment Project Management	409
12.1 Project Planning	409
12.1.1 Project Definition	409
12.1.2 Project Planning Details.....	410
12.1.2.1 Project Phases and Activities.....	410
12.1.2.2 Phases and Activities Scheduling	411
12.1.2.3 Allocating Hours to Activities	412

12.1.3	Project Resources.....	413
12.1.3.1	Objectivity vs. Independence.....	413
12.1.3.2	Internal vs. External Team Members.....	415
12.1.3.3	Skills Required	416
12.1.3.4	Team Skills.....	416
12.1.3.5	Team Member Skills.....	416
12.2	Project Tracking	424
12.2.1	Hours Tracking	424
12.2.2	Calendar Time Tracking	424
12.2.3	Project Progress Tracking	427
12.3	Taking Corrective Measures.....	428
12.3.1	Obtaining More Resources.....	428
12.3.2	Using Management Reserve	428
12.4	Project Status Reporting.....	430
12.4.1	Report Detail	430
12.4.2	Report Frequency	430
12.4.3	Status Report Content.....	431
12.5	Project Conclusion and Wrap-Up.....	431
12.5.1	Eliminating “Scope Creep”.....	431
12.5.2	Eliminating Project Run-On	432
	Exercises	432
	Notes	433
	Reference	433
13	Security Risk Assessment Approaches.....	435
13.1	Quantitative vs. Qualitative Analysis.....	436
13.1.1	Quantitative Analysis	436
13.1.1.1	Expected Loss.....	437
13.1.1.2	Single Loss Expectancy.....	437
13.1.1.3	Annualized Loss Expectancy	438
13.1.1.4	Safeguard Value.....	438
13.1.1.5	Quantitative Analysis Advantages.....	439
13.1.1.6	Quantitative Analysis Disadvantages.....	441
13.1.2	Qualitative Analysis.....	443
13.1.2.1	Qualitative Analysis Advantages.....	444
13.1.2.2	Qualitative Analysis Disadvantages	446
13.2	Tools.....	446
13.2.1	Lists.....	447
13.2.2	Templates	447
13.3	Security Risk Assessment Methods.....	447
13.3.1	FAA Security Risk Management Process.....	448
13.3.2	OCTAVE	448
13.3.3	FRAP	448

13.3.4 CRAMM451

13.3.5 NSA IAM.....451

Exercises451

Notes452

References.....452

Index.....455