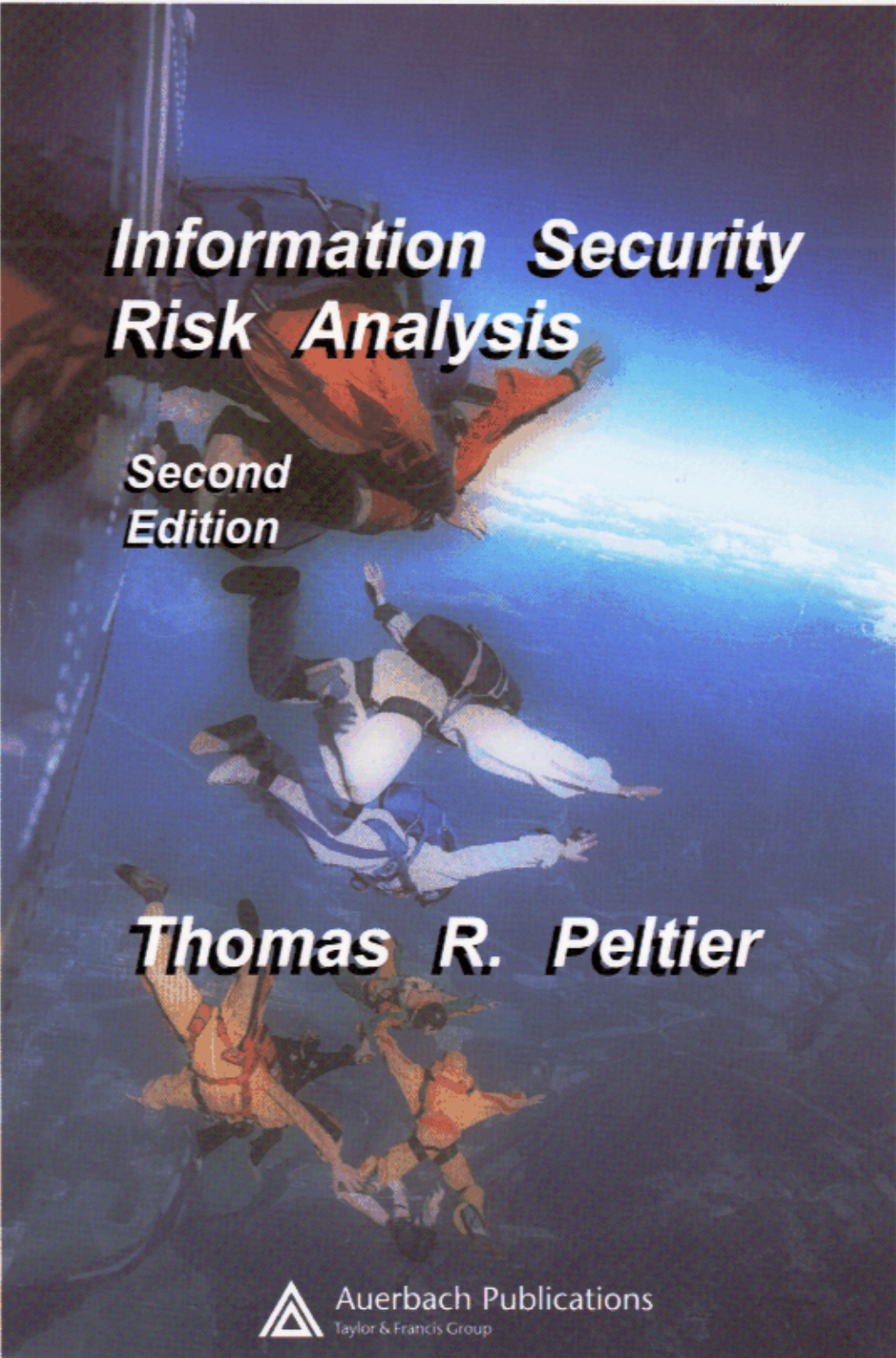


The background of the book cover is a photograph of several skydivers in freefall against a bright blue sky. The skydivers are wearing various colored jumpsuits (orange, white, blue, and tan) and are in different poses, some with arms spread wide. The perspective is from above, looking down at the divers.

Information Security Risk Analysis

***Second
Edition***

Thomas R. Peltier



Auerbach Publications
Taylor & Francis Group

Contents

1	Introduction.....	1
1.1	Frequently Asked Questions.....	2
1.1.1	Why Should a Risk Assessment Be Conducted?.....	2
1.1.2	When Should a Risk Analysis Be Conducted?	3
1.1.3	Who Should Conduct the Risk Analysis and Risk Assessment?	3
1.1.4	Who within the Organization Should Conduct the Risk Analysis and Risk Assessment?	4
1.1.5	How Long Should a Risk Analysis or Assessment Take?.....	4
1.1.6	What Can a Risk Analysis or Risk Assessment Analyze?.....	4
1.1.7	What Can the Results of a Risk Management Tell an Organization?	5
1.1.8	Who Should Review the Results of a Risk Analysis?	5
1.1.9	How Is the Success of the Risk Analysis Measured?.....	5
1.2	Conclusion.....	6
2	Risk Management	7
2.1	Overview	7
2.2	Risk Management as Part of the Business Process	8
2.3	Employee Roles and Responsibilities.....	10
2.4	Information Security Life Cycle	11
2.5	Risk Analysis Process	15
2.6	Risk Assessment.....	16
2.6.1	Step 1: Asset Definition.....	16
2.6.2	Step 2: Threat Identification	18
2.6.3	Step 3: Determine Probability of Occurrence	19
2.6.4	Step 4: Determine the Impact of the Threat.....	24
2.6.5	Step 5: Controls Recommended.....	25
2.6.6	Step 6: Documentation.....	27
2.7	Cost-Benefit Analysis.....	27
2.8	Risk Mitigation.....	38
2.9	Final Thoughts	39

3 Risk Assessment Process	41
3.1 Introduction	41
3.2 Risk Assessment Process	41
3.3 Information Is an Asset	42
3.4 Risk Assessment Methodology	44
3.4.1 Threat Identification	45
3.4.1.1 Elements of Threats	46
3.4.1.2 Threat Occurrence Rates	48
3.4.1.3 Risk Level Determination	50
3.4.1.4 Controls and Safeguards	52
3.4.1.5 Cost-Benefit Analysis	74
3.4.1.6 Documentation	74
3.5 Final Thoughts	74
4 Quantitative versus Qualitative Risk Assessment	77
4.1 Introduction	77
4.2 Quantitative and Qualitative Pros and Cons	79
4.3 Qualitative Risk Assessment Basics	79
4.3.1 Step 1: Develop a Scope Statement	81
4.3.2 Step 2: Assemble a Quality Team	81
4.3.3 Step 3: Identify Threats	84
4.3.4 Step 4: Prioritize Threats	84
4.3.5 Step 5: Threat Impact	90
4.3.6 Step 6: Risk Factor Determination	92
4.3.7 Step 7: Identify Safeguards and Controls	93
4.3.8 Step 8: Cost-Benefit Analysis	96
4.3.9 Step 9: Rank Safeguards in Recommended Order	96
4.3.10 Step 10: Risk Assessment Report	97
4.3.11 Summary	99
4.4 Qualitative Risk Assessment Using Tables	99
4.4.1 Stage 1: Asset Valuation (BIA)	101
4.4.2 Stage 2: Risk Evaluation	102
4.4.3 Stage 3: Risk Management	107
4.4.4 Summary	108
4.5 The 30-Minute Risk Assessment	108
4.5.1 Overview	108
4.5.2 Objectives	108
4.5.3 ISRA Matrix	109
4.5.4 The ISRA Process	109
4.5.5 Threat-Based Controls	111
4.5.6 Documentation	112
4.5.7 Out-of-Control Process	113
4.5.8 Final Notes	113
4.6 Conclusion	114

5 Other Forms of Qualitative Risk Assessment	115
5.1 Introduction	115
5.2 Hazard Impact Analysis	116
5.2.1 Hazard Impact Analysis Process	116
5.2.2 Paralysis by Analysis	119
5.3 Questionnaires	120
5.3.1 Risk Assessment Questionnaire Process	121
5.3.2 Summary	124
5.4 Single Time Loss Algorithm	124
5.5 Conclusion	125
6 Facilitated Risk Analysis and Assessment Process (FRAAP)	129
6.1 Introduction	129
6.2 FRAAP Overview	129
6.3 Why the FRAAP Was Created	131
6.4 Introducing the FRAAP to Your Organization	132
6.4.1 Awareness Program Overview	133
6.4.2 Introducing the FRAAP	134
6.4.3 Facilitation Skills	136
6.4.3.1 Listen	136
6.4.3.2 Lead	137
6.4.3.3 Reflect	137
6.4.3.4 Summarize	137
6.4.3.5 Confront	137
6.4.3.6 Support	138
6.4.3.7 Crisis Intervention	138
6.4.3.8 Center	138
6.4.3.9 Solve Problems	139
6.4.3.10 Change Behavior	139
6.4.3.11 Recognize All Input and Encourage Participation	139
6.4.3.12 Be Observant for Nonverbal Responses	139
6.4.3.13 Do Not Lecture; Listen and Get the Team Involved	140
6.4.3.14 Never Lose Sight of the Objective	140
6.4.3.15 Stay Neutral (or Always Appear to Remain Neutral)	140
6.4.3.16 Learn to Expect Hostility, but Do Not Become Hostile	140
6.4.3.17 Avoid Being the Expert Authority	140
6.4.3.18 Adhere to Time Frames and Be Punctual	141
6.4.3.19 Use Breaks to Free a Discussion	141
6.4.3.20 The Facilitator Is There to Serve the FRAAP Team	141
6.4.3.21 Stop the FRAAP if the Group Is Sluggish and Difficult to Control	141
6.4.4 Session Agreements	143

6.4.5	The FRAAP Team	144
6.4.6	Prescreening	147
6.4.6.1	Prescreening Example 1	147
6.4.6.2	Prescreening Example 2	153
6.4.6.3	Prescreening Example 3	155
6.4.7	The Pre-FRAAP Meeting	159
6.4.7.1	Pre-FRAAP Meeting Process	159
6.4.7.2	Pre-FRAAP Summary	165
6.4.8	The FRAAP Session	166
6.4.8.1	The FRAAP Session Stage 1	166
6.4.8.2	The FRAAP Session Stage 2	182
6.4.8.3	FRAAP Session Summary	183
6.4.9	The Post-FRAAP	186
6.4.9.1	Complete Action Plan	186
6.4.9.2	FRAAP Management Summary Report	190
6.4.9.3	Cross-Reference Report	194
6.4.9.4	Summary	203
6.5	Conclusion	204
7	Variations on the FRAAP	205
7.1	Overview	205
7.2	Infrastructure FRAAP	205
7.2.1	The Infrastructure FRAAP	206
7.2.1.1	Infrastructure FRAAP Summary	207
7.2.2	Application FRAAP	212
7.2.2.1	Overview	212
7.2.2.2	Summary	212
7.2.3	Other Variations	213
7.2.3.1	Variation Example 1	213
7.2.3.2	Variation Example 2	213
7.2.3.3	Variation Example 3	218
7.3	Conclusion	221
8	Mapping Controls	223
8.1	Controls Overview	223
8.2	Creating Your Controls List	224
8.2.1	Information Security Baseline Controls	224
8.2.2	Control Requirements Considerations	226
8.2.3	A Final Cautionary Note	226
8.3	Controls List Examples	227
8.3.1	Controls by Security Categories	227
8.3.2	Controls List by Information Security Layer	228
8.3.3	Controls List by Information Technology Organization	229
8.3.4	Controls List Using ISO 17799	229
8.3.5	Mapping ISO 17799 and HIPAA	236
8.3.6	Controls List Mapping ISO 17799 and GLBA	236

8.3.7 Controls List Mapping ISO 17799, GLBA, and Sarbanes-Oxley	245
8.3.8 Controls List Mapping ISO 17799 and Federal Sentencing Guidelines	245
8.3.9 Controls List Mapping ISO 17799, HIPAA, GLBA, SOX, and FSGCA	249
8.3.10 National Institute of Standards and Technology Controls List	249
8.3.11 Controls List Mapping ISO 17799 and CobIT	250
8.3.12 Other Sources	261
9 Business Impact Analysis (BIA)	289
9.1 Overview	289
9.2 Creating a BIA Process	290
10 Conclusion	297
Appendix A: Sample Risk Assessment Management Summary Report	299
Appendix B: Terms and Definitions	325
Appendix C: Bibliography	331
Index	335