

# Contents

<b>Introduction</b>	<b>xxv</b>
<b>Chapter 1 Laying the Foundation for Your Assessment</b>	<b>1</b>
Introduction	2
Determining Contract Requirements	3
What Does the Customer Expect?	4
Customer Definition of an Assessment	4
Sources for Assessment Work	7
Contract Composition	7
What Does the Work Call For?	11
What Are the Timelines?	16
Understand the Pricing Options	18
Understanding Scoping Pitfalls	20
Common Areas of Concern	21
Customer Concerns	21
Customer Constraints	21
“Scope Creep” and Timelines	22
Uneducated Salespeople	23
Bad Assumptions	24
Poorly Written Contracts	25
Staffing Your Project	27
Job Requirements	27
Networking and Operating Systems	27
Hardware Knowledge	28
Picking the Right People	28
Adequately Understanding Customer Expectations	30
The Power of Expectations	30
What Does the Customer Expect for Delivery?	30
Adjusting Customer Expectations	30
	xi

Educating the Customer	31
Helping the Customer Understand the Level of Effort	31
Explaining Timeline Requirements	31
Understand the Commitment	32
Project Leadership	32
Constant Communication with the Customer	32
Constant Communication with Team Members	33
Timeliness of the Effort	34
Long Nights, Impossible Odds	35
Initial Resistance Fades to Cooperation	35
Case Study: Scoping Effort for the Organization for Optimal Power Supply	36
Summary	39
Best Practices Checklist	40
Frequently Asked Questions	42
<b>Chapter 2 The Pre-Assessment Visit</b>	<b>45</b>
Introduction	46
Preparing for the Pre-Assessment Visit	47
Questions You Should Ask	48
Determining the Network Environment of the Assessment Site	48
Determining the Security Controls of the Assessment Site	50
Understanding Industry Concerns for the Assessment Site	50
Scheduling	52
Understanding Special Considerations	53
Managing Customer Expectations	53
Defining the Differences Between Assessment and Audit	54
Results, Solutions, and Reporting	56
Interference on Ops	57
Impact on Organization Security	58
Defining Roles and Responsibilities	60
Who Is the Decision Maker?	61

Who Is the Main Customer POC?	61
Who Is the Assessment Team Leader?	62
Suggestions for the Assessment Team	63
Possible Members of the Customer Team	63
Planning for the Assessment Activities	65
Developing Mission Identification	66
Understanding Industry Differences	67
Relating the Mission to Pre-Assessment Site Visit Products	68
Defining Goals and Objectives	69
Understanding the Effort: Setting the Scope	69
Information Request	69
Coordinate	70
Establish Team Needs for Remaining Assessment	70
Industry and Technical Considerations	70
Case Study: The Bureau of Overt Redundancy	71
The Organization	71
Summary	75
Best Practices Checklist	76
Frequently Asked Questions	77
<b>Chapter 3 Determining the Organization's Information Criticality</b>	<b>81</b>
Introduction	82
Identifying Critical Information Topics	86
Associating Information Types with the Mission	90
Common Issues in Defining Types	91
Common Mistakes in Defining Types	92
Identifying Impact Attributes	93
Common Impact Attributes	95
Confidentiality	96
Integrity	96
Availability	96
Additional Impact Attributes	97
Based on Regulatory or Legal Requirements	97
Personal Preference	98
Recommendation of a Colleague	99

Creating Impact Attribute Definitions	99
Understanding the Impact to the Organization	99
Can We Live Without This Information?	100
Example Impact Definitions	100
High, Medium, and Low	100
Numbered Scales	103
Creating the Organizational Information	
Criticality Matrix	104
Prioritizing Impact Based on Your Definitions	105
The Customer Perception of the Matrix	107
Case Study: Organizational Criticality at TOOT	108
TOOT Information Criticality Topics	109
Identifying Impact Attributes	110
Creating Impact Definitions	110
Creating the Matrix	111
Summary	113
Best Practices Checklist	115
Frequently Asked Questions	116
<b>Chapter 4 System Information Criticality</b>	<b>119</b>
Introduction	120
Stepping into System Criticality	121
Defining High-Level Security Goals	123
Locating Additional Sources of Requirements	126
Determining System Boundaries	128
Physical Boundaries	128
Logical Boundaries	128
Defining the Systems	130
What Makes a System Critical?	132
Breaking the Network into Systems	133
What Makes Sense?	134
Creating the System Criticality Matrix	134
The Relationship Between OICM and SCM	135
Refining Impact Definitions	136
A Matrix for Each System	137
Unexpected Changes	138
Case Study: Creating the SCM for TOOT	140

Locating System Boundaries	140
Completing the System Criticality Matrix	141
Summary	145
Best Practices Checklist	147
Frequently Asked Questions	149
<b>Chapter 5 The System Security Environment</b>	<b>151</b>
Introduction	152
Understanding the Cultural and Security Environment	154
The Importance of Organizational Culture	154
Adequately Identifying the Security Environment	156
Defining the Boundaries	159
Physical Boundaries	160
Logical Boundaries	161
Never the Twain Shall Meet—Or Should They?	162
Identifying the Customer Constraints and Concerns	162
Defining Customer Constraints	163
Types of Operational Constraints	163
Types of Resource Constraints	164
Environmental Constraints	164
Architectural Constraints	165
Determining Customer Concerns	166
Why Are You There in the First Place?	166
Specific Criteria to Assess	166
Handling the Documentation Identification and Collection	167
What Documentation Is Necessary?	169
Policy	169
Guidelines/Requirements	169
Plans	170
Standard Operating Procedures	170
User Documentation	170
Obtaining the Documentation	171
Use the Customer Team Member	171
Tracking the Documents	171
Determining Documentation Location	172
What If No Documentation Exists?	172
Ad Hoc Security	173

Case Study: Higher Education	174
Summary	179
Best Practices Checklist	179
Frequently Asked Questions	181
<b>Chapter 6 Understanding the Technical Assessment Plan</b>	<b>183</b>
Introduction	184
Understanding the Purpose of the Technical Assessment Plan	184
The TAP: A Plan of Action	187
The TAP: A Controlled and Living Document	187
Linking the Plan to Contract Controls	188
Understanding the Format of the TAP	190
Point of Contact	191
Mission	192
Organizational Information Criticality	193
System Information Criticality	194
Customer Concerns and Constraints	195
System Configuration	196
Interviews	197
Documents	198
Timeline of Events	200
Customizing and Modifying the TAP to Suit the Job at Hand	200
Modifying the Nine NSA-Defined Areas	201
Level of Detail	201
Format	202
Case Study: The Bureau of Overt Redundancy	202
The BOR TAP	202
Contact Information	203
Mission	204
Organization Information Criticality	206
System Information Criticality	208
Concerns and Constraints	209
System Configuration	209
The Interview List	210

Documentation	211
Events Timeline	213
Summary	215
Best Practices Checklist	216
Frequently Asked Questions	217
<b>Chapter 7 Customer Activities</b>	<b>219</b>
Introduction	220
Preparing for the Onsite Phase	220
Assessment Team Preparation	221
Administrative Planning	222
Technical Planning	223
Customer Preparation	224
Scheduling	225
Communication	225
Setting the Onsite Tone	226
Understanding the Opening Meeting (The Inbriefing)	227
Conducting the Opening Meeting	228
Meeting Format	228
Information to Take Away	228
Establishing and Maintaining the Onsite Expectations	229
Understanding the Process	229
Understanding the Results	230
Keeping the Customer Involved	230
Continued Customer Education	230
Information Exchange	231
NSA IAM Baseline INFOSEC Classes and Categories	232
Management Aspects	233
INFOSEC Documentation	234
INFOSEC Roles and Responsibilities	234
Contingency Planning	235
Configuration Management	236
Technical Aspects	236
Identification and Authentication	237
Account Management	238
Session Controls	239
Auditing	240

Malicious Code Protection	240
Maintenance	241
System Assurance	241
Networking/Connectivity	242
Communications Security	243
Operational Aspects	243
Media Controls	243
Labeling	244
Physical Environment	244
Personnel Security	245
Education Training and Awareness	245
The Fine Art of the Interview	246
Interview Characteristics	246
Whom Do I Interview?	247
Interview Scheduling	248
Interview Environment	248
Attributes of a Successful Interviewer	249
Breaking the Barriers	249
Gaining Needed Information	252
Case Study: Interviews With University Staff	254
The Management Interview	258
The Technical Interview	260
Group Interview with Computer Science Systems Administrators	260
Individual Interview with Marcia	262
Summary	264
Best Practices Checklist	265
Frequently Asked Questions	266
<b>Chapter 8 Managing the Findings</b>	<b>269</b>
Introduction	270
Demonstration Versus Evaluation	271
What Are System Demonstrations?	271
The Good and the Bad	272
What Are System Evaluations?	273
Manual Checks	274
Tailored Scripts	274

Tools	274
Findings and Dependencies	276
When Is a Finding Considered Dependent?	277
Is It Good or Bad? Does It Matter?	278
Mapping Findings to Requirements and Constraints	278
Justification	279
Mapping Requirements	280
Creating Recommendation Road Maps	281
Cost Effectiveness	281
Applicability	281
Importance	282
Users	282
Options for Increasing the Security Posture	282
The Yugo Implementation	283
The Ford Solution	284
The Cadillac Solution	284
Case Study: Medical Management	284
System Description	286
Information Criticality	286
Summary of Findings	287
Excerpt of Findings	288
Recommendation Road Map	298
Summary	305
Best Practices Checklist	305
Frequently Asked Questions	307
<b>Chapter 9 Leaving No Surprises</b>	<b>309</b>
Introduction	310
Determining the Audience for the Closeout Meeting	310
Who Is Your Audience?	311
Who Should Attend?	311
Organizing the Closeout Meeting	312
Determining Time and Location	312
Time of Meeting	313
Day of Week	313
Meeting Room	313
Determining Supply List for the Closeout Meeting	313

Other Concerns about the Meeting	314
Understanding the Meeting Agenda	314
Review of the Assessment Plan	315
Review of Organization Information Criticality	315
Systems Information Criticality	316
Customer Concerns and Constraints	318
Reviewing Goals, Purpose, and Scope	319
Reviewing the Critical Vulnerabilities	319
Findings	320
Discussion	320
Recommendation(s)	321
Reviewing the Process and Looking Forward	321
Who Was Involved?	321
What Has Been Done?	321
How Much Time Did it Take?	322
What Happens Next?	322
Who Should Be Involved?	322
What Can the Customer Expect in the	
Final Report?	322
We Came, We Saw, Now What?	322
What Happens Next?	323
Who Needs to Be Involved?	323
How Things Progress from Here	323
When Can the Client Expect a Finished Product?	323
Case Study: Software Creation and Solutions Inc. (SCS)	324
Summary	329
Best Practices Checklist	329
Frequently Asked Questions	331
<b>Chapter 10 Final Reporting</b>	<b>333</b>
Introduction	334
Preparing for Analysis	334
Consolidating and Correlating Assessment Information	334
Assessment Team Meetings	335
Assessment Team Writing Assignments	335
Review of Assessment Information	336
Understanding Findings (Doing the Analysis)	336

What Is Risk?	336
Analysis Objectives	338
Verify Perceived Vulnerabilities	338
Identify Additional Vulnerabilities	339
New Critical Findings	339
Previously Identified Critical Findings	340
Communicating with the Customer	340
Determine the Customer's Security Posture	340
Environmental Threats	341
Human Threats	341
Vulnerability Classification	342
Positive Findings	342
Negative Findings	342
Multiple Recommendations for Each Finding	344
Creating and Formatting the Final Report	345
Executive Summary	346
Executive Summary Content	346
Introduction	347
Customer and Assessment Company Information	348
Assessment Process Description	348
Purpose of the Assessment	349
System Description	349
The Customer's Mission Is Important	349
Information Criticality	349
System Criticality	350
Actual System Description	350
A Picture Is Worth a Thousand Words	350
INFOSEC Analysis	351
Topic Areas	351
Identifying the Findings	352
Discussion of the Findings	352
Recommendations for Improving Security Posture	352
Conclusion	353
Delivering the Final Report	354
Cover Letter	354
Attach the Assessment Plan	354

Customer Acknowledgment	355
Case Study: Analyzing Findings for Important Internet Services Provided, Inc.	355
Executive Summary	356
Organizational Assessment Findings Summary	356
INFOSEC Analysis	357
Organizational Assessment Findings	357
High-Severity Findings	358
Medium-Severity Findings	360
Conclusion	361
Results	362
Summary	363
Best Practices Checklist	364
Frequently Asked Questions	365
<b>Chapter 11 Tying Up Loose Ends</b>	<b>367</b>
Introduction	368
Examining Document Retention	368
Public Domain Documentation	369
Customer Documentation	370
Documentation Generated by the Assessment Team	370
Controlling What Is Retained	372
Contract Concerns	373
Liability Concerns	375
Other Retention Concerns	376
Performing Customer Followup	377
Understanding the Followup Process	380
Showing Adequate Concern	380
Utilizing Multiple Means for Followup	383
Asking the Right Questions	383
Designating Responsibility for Following Up	384
Tracking the Followup Process	385
Evaluating Lessons Learned	386
Understanding the Value of Lessons Learned	387
Why Are Lessons Learned So Important?	387
Identifying Lessons Learned	388
What Have We Learned Here?	388

Utilizing Lessons Learned	390
Integrating Lessons Learned into the Business Process	390
Making It Repeatable	392
Case Study: The University of Science	393
Understanding the Requirements	393
What Should We Keep?	393
What Should We Destroy?	394
Designating a Followup POC	394
What Have We Learned?	395
Summary	396
Best Practices Checklist	397
Frequently Asked Questions	398
<b>Appendix A Forms, Worksheets, and Templates</b>	<b>401</b>
IAM Pre-Assessment Site Visit Checklist	402
IAM Planning Survey	404
Types of Documents That Require Tracking	408
Policy Documents	408
Guideline/Requirements Documents	409
System Security Plan Documents	409
User Documents	410
Document-Tracking Templates	411
Elements of the Technical Assessment Plan	412
The Interview List	413
The Assessment Timeline	414
<b>Index</b>	<b>417</b>