

Contents

Foreword	xxiii
Preface	xxv
Chapter 1 What Is Certification and Accreditation?	1
Introduction	.2
Terminology	.3
Audit and Report Cards	.6
A Standardized Process	.7
Templates, Documents, and Paperwork	.8
Certification and Accreditation Laws Summarized	.9
Summary	.10
Notes	.11
Chapter 2 Types of Certification and Accreditation . . .	13
Introduction	.14
The NIACAP Process	.15
The NIST Process	.16
NIACAP and NIST Phases, Differences, and Similarities .16	
NIACAP and NIST Compared	.17
DITSCAP	.18
DCID 6/3	.19
The Common Denominator of All C&A Methodologies . .	.20
C&A for Private Enterprises	.21
Summary	.23
Notes	.23
Chapter 3 Understanding the Certification and Accreditation Process	25
Introduction	.26
Recognizing the Need for C&A	.26
Roles and Responsibilities	.27
Chief Information Officer	.27
Authorizing Official	.29
Senior Agency Information Security Officer	.30

- Senior Agency Privacy Official 31
- Certification Agent/Evaluation Team 31
- Business Owner 33
- System Owner 33
- Information Owner 33
- Information System Security Officer 34
- C&A Preparers 35
- Agency Inspectors 35
- GAO Inspectors 36
- Levels of Audit 36
- Stepping through the Process 37
 - The Initiation Phase 37
 - The Certification Phase 40
 - The Accreditation Phase 41
 - The Continuous Monitoring Phase 42
- Summary 44
- Chapter 4 Establishing a C&A Program..... 45**
 - Introduction 46
 - C&A Handbook Development 46
 - What to Include in Your Handbook 47
 - Who Should Write the Handbook? 48
 - Template Development 48
 - Provide Package Delivery Instructions 50
 - Create an Evaluation Process 51
 - Authority and Endorsement 51
 - Improve Your C&A Program Each Year 52
 - Problems of Not Having a C&A Program 52
 - Missing Information 52
 - Lack of Organization 53
 - Inconsistencies in the Evaluation Process 53
 - Unknown Security Architecture and Configuration ... 53
 - Unknown Risks 54
 - Laws and Report Cards 54
 - Summary 55

Chapter 5 Developing a Certification Package	57
Introduction	.58
Initiating Your C&A Project	.58
Put Together a Contact List	.58
Hold a Kick-Off Meeting	.59
Obtain Any Existing Agency Guidelines	.60
Analyze Your Research	.61
Preparing the Documents	.61
It's Okay to Be Redundant	.62
Different Agencies Have Different Requirements	.62
Including Multiple Applications and Systems in One Package	.63
Verify Your Information	.64
Retain Your Ethics	.64
Summary	.66
Chapter 6 Preparing the Hardware and Software Inventory	67
Introduction	.68
Determining the Accreditation Boundaries	.68
Collecting the Inventory Information	.70
Structure of Inventory Information	.71
Delivery of Inventory Document	.72
Summary	.74
Chapter 7 Determining the Certification Level	75
Introduction	.76
What Are the C&A Levels?	.76
Level 1	.76
Level 2	.77
Level 3	.77
Level 4	.78
Importance of Determining the C&A Level	.79
Don't Make This Mistake	.79
Criteria to Use for Determining the Levels	.81
Confidentiality, Integrity, and Availability	.81
Confidentiality	.82

- Determining the Confidentiality Level83
- Integrity84
 - Determining the Integrity Level84
- Availability85
 - Determining the Availability Level86
- How to Categorize Multiple Data Sets86
- Impact Levels and System Criticality87
- System Attribute Characteristics89
 - Interconnection State (Interfacing Mode)89
 - Access State (Processing Mode)90
 - Accountability State (Attribution Mode)91
 - Mission Criticality92
- Determining Level of Certification93
- Template for Levels of Determination94
- Rationale for the Security Level Recommendation97
- Process and Rationale for the C&A Level Recommendation 99
- The Explanatory Memo102
 - Template for Explanatory Memo103
- Summary105

Chapter 8 Performing and Preparing the Self-Assessment 107

- Introduction108
- Objectives108
- Designing the Survey109
 - Levels of Compliance109
 - Management Controls111
 - Operational Controls112
 - Technical Controls113
 - Correlation with Security Policies and Laws113
 - Answering the Questions114
- Questions for Self-Assessment Survey116
- Summary137
- Notes138

Chapter 9 Addressing Security Awareness and Training Requirements 139

- Introduction140

Purpose of Security Awareness and Training	140
Security Training	141
Security Awareness	142
The Awareness and Training Message	142
Online Training Makes It Easy	144
Document Your Plan	144
Security Awareness and Training Checklist	145
Security Awareness Material Evaluation	145
Security Awareness Class Evaluation	147
Summary	148
Notes	148

Chapter 10 Addressing End-User Rules of Behavior . . 149

Introduction	150
Implementing Rules of Behavior	150
What Rules to Include	151
Rules for Applications, Servers, and Databases	151
Additional Rules for Handhelds	152
Additional Rules for Laptops and Desktop Systems	153
Additional Rules for Privileged Users	154
Consequences of Noncompliance	155
Rules of Behavior Checklist	155
Summary	156

Chapter 11 Addressing Incident Response 157

Introduction	158
Purpose and Applicability	158
Policies and Guidelines	159
Reporting Framework	160
Roles and Responsibilities	162
Agency CSIRC	162
Information System Owner and ISSO	163
Incident Response Manager	164
Definitions	165
Incident	165
Impact, Notification, and Escalation	166
Incident Handling	168

Detecting an Incident	169
Containment and Eradication	171
Recovery and Closure	172
Forensic Investigations	173
Incident Types	176
Incident Response Plan Checklist	180
Security Incident Reporting Form	181
Summary	183
Additional Resources	183
Incident Response Organizations	183
Additional Resources	184
Articles and Papers on Incident Response	185
Notes	186

Chapter 12 Performing the Security Tests and Evaluation 187

Introduction	188
Types of Security Tests	188
Confidentiality Tests	189
Integrity Tests	191
Availability Tests	192
Types of Security Controls	193
Management Controls	193
Operational Controls	194
Technical Controls	194
Testing Methodology and Tools	194
Algorithm Testing	197
Code and Memory Analyzers	198
Network and Application Scanners	199
Port Scanners	200
Port Listeners	201
Modem Scanners	201
Wireless Network Scanner	202
Wireless Intrusion Detection Systems	202
Wireless Key Recovery	203
Password Auditing Tools	203
Database Vulnerability Testing Tools	204

Test Management Packages	204
Who Should Perform the Tests?	205
Documenting the Tests	205
Analyzing the Tests and Their Results	205
Summary	207
Additional Resources	207
Books Related to Security Testing	207
Articles and Papers Related to Security Testing	208
Notes	209

Chapter 13 Conducting a Privacy Impact Assessment 211

Introduction	212
Privacy Laws, Regulations, and Rights	212
OMB Memoranda	213
Laws and Regulations	213
PIA Answers Questions	214
Personally Identifiable Information (PII)	215
Persistent Tracking Technologies	217
Determine Privacy Threats and Safeguards	218
Decommissioning of PII	219
System of Record Notice (SORN)	220
Posting the Privacy Policy	220
PIA Checklist	220
Summary	222
Books on Privacy	222
Notes	222

Chapter 14 Performing the Business Risk Assessment 225

Introduction	226
Determine the Mission	227
Create a Mission Map	229
Construct Risk Statements	230
Describe the Sensitivity Model	232
Impact Scale	233
Likelihood Scale	234
Calculating Risk Exposure	234
Lead the Team to Obtain the Metrics	235
Analyze the Risks	235

Make an Informed Decision237

 Accept the Risk237

 Transfer the Risk238

 Mitigate the Risk238

Summary241

Books and Articles on Risk Assessment241

Notes242

Chapter 15 Preparing the Business Impact Assessment 243

Introduction244

Document Recovery Times244

Establish Relative Recovery Priorities245

 Telecommunications246

 Infrastructure Systems247

 Secondary Systems247

Define Escalation Thresholds248

Record License Keys249

BIA Organization250

Summary252

Additional Resources252

Chapter 16 Developing the Contingency Plan 253

Introduction254

List Assumptions255

Concept of Operations255

 System Description255

 Network Diagrams and Maps256

 Data Sources and Destinations256

Roles and Responsibilities257

 Contingency Planning Coordinator258

 Damage Assessment Coordinator259

 Emergency Relocation Site Adviser and Coordinator260

 Information Systems Operations Coordinator260

 Logistics Coordinator260

 Security Coordinator261

 Telecommunications Coordinator261

Levels of Disruption	262
Procedures	263
Backup and Restoration Procedures	263
Procedures to Access Off-site Storage	264
Operating System Recovery Procedures	264
Application Recovery Procedures	265
Connectivity Recovery Procedures	265
Key Recovery Procedures	266
Power Recovery Procedures	266
Recovering and Assisting Personnel	267
Notification and Activation	267
Line of Succession	269
Service Level Agreements	269
Contact Lists	270
Testing the Contingency Plan	270
Appendices	271
Contingency Plan Checklist	271
Additional Resources	272

Chapter 17 Performing a System Risk Assessment . . . 275

Introduction	276
Risk Assessment Creates Focus	276
Determine Vulnerabilities	278
Threats	280
Threats Initiated by People	280
Threats Initiated by Computers or Devices	280
Threats from Natural Disasters	281
Qualitative Risk Assessment	282
Quantitative Risk Assessment	283
Qualitative versus Quantitative Risk Assessment	287
Present the Risks	288
Make Decisions	291
Checklist	291
Summary	293
Additional Resources	293
Notes	294

Chapter 18 Developing a Configuration Management Plan 295

 Introduction 296

 Establish Definitions 296

 Describe Assets Controlled by the Plan 297

 Describe the Configuration Management System 298

 Define Roles and Responsibilities 299

 Establish Baselines 301

 Change Control Process 302

 Change Request Procedures 303

 Emergency Change Request Procedures 303

 Change Request Parameters 304

 Configuration Control Board 304

 Configuration Management Audit 306

 Configuration and Change Management Tools 307

 Configuration Management Plan Checklist 308

 Summary 309

 Additional Resources 309

Chapter 19 Preparing the System Security Plan 311

 Introduction 312

 Laws, Regulations, and Policies 312

 The System Description 313

 System Boundaries 315

 System Mission 316

 Data Flows 318

 Security Requirements and Controls 318

 Management Controls 325

 Risk Mitigation 325

 Reporting and Review by Management 326

 System Lifecycle Requirements 328

 Security Planning 329

 Documentation for Managers 329

 Operational Controls 330

 Personnel Security 330

 Physical and Environmental Controls and Safeguards 331

 Administration and Implementation 332

Preventative Maintenance	333
Contingency and Disaster Recovery Planning	334
Training and Security Awareness	334
Incident Response Procedures	335
Preservation of Data Integrity	335
Network and System Security Operations	336
Technical Controls	338
Authentication and Identity Verification	338
Logical Access Controls	341
Secure Configurations	341
Interconnectivity Security	344
Audit Mechanisms	346
ISSO Appointment Letter	349
System Security Plan Checklist	351
Summary	353
Additional Resources	353
Notes	354
Chapter 20 Submitting the C&A Package	355
Introduction	356
Structure of Documents	356
Who Puts the Package Together?	357
Markings and Format	357
Signature Pages	358
A Word About “Not Applicable” Information	359
Submission and Revision	360
Defending the Certification Package	360
Checklist	362
Summary	363
Additional Resources	363
Chapter 21 Evaluating the Certification Package for Accreditation.	365
Introduction	366
The Security Assessment Report	366
Checklists for Compliance	366
Compliance Checklist for Management Controls	368

- Compliance Checklist for Operational Controls 380
- Compliance Checklist for Technical Controls 392
- Recommendation to Accredite or Not 404
- Accreditation and Authority to Operate 405
- Interim Authority to Operate 405
- Evaluations by an OIG 407
- Evaluations by the GAO 408
- Checklist 409
- Summary 410
- Chapter 22 Addressing C&A Findings 411**
 - Introduction 412
 - POA&Ms 412
 - Development and Approval 412
 - POA&M Elements 413
 - A Word to the Wise 416
 - Checklist 416
 - Summary 417
- Chapter 23 Improving Your
Federal Computer Security Report Card Scores 419**
 - Introduction 420
 - Elements of the Report Card 420
 - Actions for Improvement 421
 - Trends 422
 - Summary 423
- Chapter 24 Resources 425**
 - Acronyms 428
- Appendix A FISMA 431**
- Appendix B OMB Circular A-130: Appendix III 453**
- Appendix C FIPS 199 473**
- Index. 485**