

CONTENTS

| | |
|--|------------|
| Introduction | 1 |
| Purpose and scope | 1 |
| Motivation – what do we hope to accomplish with this book? | 2 |
| Who is the target audience? | 4 |
| Terminology | 5 |
| Overview of the contents | 6 |
| Chapter 1: An Abridged History of Information Technology and Information Systems Security | 9 |
| From physical to virtual – a highly abridged history of information technology | 10 |
| Information systems and information systems security – merging concerns | 13 |
| Chapter 2: The Essential Information Systems Security Regulations | 19 |
| Information systems security regulations you need to know | 20 |
| Chapter 3: The Authorization Process Framework | 71 |
| Commonly found authorization process deficiencies | 72 |
| Authorization process commonalities | 75 |
| The basic authorization framework..... | 77 |
| Factors that influence authorization activities | 78 |
| Joint or reciprocal authorization | 79 |
| Chapter 4: The Authorization Process – Establishing a Foundation | 83 |
| Authorization is only one part of an effective security program . | 84 |
| Designing an effective information security program | 88 |
| Milestones from the “establishing a foundation” activities | 111 |
| Chapter 5: Pre-Authorization Activities – The Fundamentals | 113 |
| Establish the authorization team | 114 |
| Training the authorization team should not be an afterthought . | 119 |
| Categorizing the information system | 120 |
| Defining the boundary ensures manageable and measurable authorization..... | 129 |
| Establishing a risk management process | 135 |
| <i>Contents</i> <i>xii</i> | |
| Align with the system life cycle (SLC) | 175 |
| Milestones from the pre-certification and accreditation activities: | 176 |
| Chapter 6: Plan, Initiate and Implement Authorization – Preparing for Authorization | 179 |
| UNDERSTAND the information and the information system .. | 181 |
| REGISTER the information system | 211 |
| NEGOTIATE the authorization approach | 215 |
| IMPLEMENT the security controls | 219 |
| Milestones from the plan, initiate, and implement authorization activities | 226 |
| Chapter 7: Verify, Validate & Authorize – Conducting the Authorization | 229 |

| | |
|--|------------|
| ASSESS the security controls | 231 |
| DEVELOP the plan of action and milestones (POA&M) | 273 |
| AUTHORIZE the operation of the information system..... | 281 |
| Milestones from the verify, validate and authorize activities | 291 |
| Chapter 8: Operate & Maintain – Maintaining Authorization | 295 |
| MONITOR the security control status: situational awareness ... | 297 |
| CONDUCT the annual review and security reporting | 303 |
| MAINTAIN the authorization | 306 |
| Milestones from the operate and maintain activities | 307 |
| Chapter 9: Remove the Information system From Operation | 309 |
| Required actions when removing an information system from operation..... | 310 |
| Avoiding self-inflicted security issues through effective system removal..... | 312 |
| Methods of removing an information system and/or its data from operation..... | 314 |
| Chapter 10: Authorization Package and Supporting Evidence | 319 |
| The authorization package in detail | 320 |
| Supporting evidence for the authorization decision – security control documentation..... | 344 |
| Chapter 11: C&A in the US Department of Defense | 403 |
| Introduction to the DIACAP | 405 |
| <i>Contents</i> | |
| <i>xiii</i> | |
| DIACAP governance structure | 415 |
| A DIACAP roadmap (guide to the stages or activities) | 418 |
| DIACAP support tools | 465 |
| C&A and the DOD components | 469 |
| Chapter 12: Authorization in the Federal Government | 473 |
| Establishing information system authorization boundaries (also known as accreditation boundaries) | 474 |
| Choose the proper accreditation vehicle | 478 |
| Security authorization process | 480 |
| Chapter 13: The Federal information Security Management Act (FISMA) | 505 |
| The e-Government Act of 2002 and FISMA | 507 |
| The FISMA report card | 508 |
| FISMA misunderstood – What FISMA is NOT | 514 |
| FISMA and its achievements | 516 |
| 10 critical questions for FISMA compliance | 518 |
| The 30,000 foot view of FISMA compliance | 519 |
| Chapter 14: Authorization and the System Life Cycle (SLC) | 521 |
| Phases of the system life cycle (SLC) | 524 |
| Life cycle phases and documentation | 529 |
| Chapter 15: Information Systems Security Training and Certification | 531 |
| Leverage your most important asset | 532 |
| The drivers | 532 |

| | |
|--|------------|
| Security education, training, and awareness (SETA) – and certification | 533 |
| Chapter 16: The Future – Revitalizing and Transforming C&A | |
| | 541 |
| Why transform?..... | 542 |
| Goals of the transformation | 542 |
| The transformation process | 545 |
| Proposed approach to C&A | 548 |
| Status of the C&A transformation | 551 |
| Transition | 552 |
| What is the value added by the transformation? | 558 |
| <i>Contents</i> | |
| <i>xiv</i> | |
| The Resource CD | 561 |
| Glossary | 573 |
| Acronyms | 583 |
| ITG Resources | 590 |