The CISSP® and CAP™
Prep Guide:
Platinum Edition

Ronald L. Krutz, Ph.D.
P.E., CISSP, ISSEP
Russell Dean Vines
CISSP, CISM, Security +, CCNA,
MCSE, MCNE

Wiley Publishing, Inc.
The CISSP® and CAP™
Prep Guide:
Platinum Edition
The CISSP® and CAP™ Prep Guide: Platinum Edition

Ronald L. Krutz, Ph.D.
P.E., CISSP, ISSEP
Russell Dean Vines
CISSP, CISM, Security +, CCNA,
MCSE, MCNE

Wiley Publishing, Inc.
Dedicated to all the hours spent in play and new discoveries of this world through the eyes of my grandchildren in their innocence, honesty, and lack of skepticism.

To: Emma, Aaron, Ryan, and Patrick

—R.L.K

Dedicated to all those who seek to make the Internet safe, private, and open to all.

—R.D.V.
RONALD L. KRUTZ, Ph.D., P.E., CISSP, ISSEP. Dr. Krutz is the Chief Knowledge Officer of Cybrinth, LLC, a firm that provides innovative information protection, analysis, assurance, and management services to government and the commercial sector. Prior to this position, Dr. Krutz was a Senior Information Security Researcher in the Advanced Technology Research Center of Lockheed Martin/Sytex, Inc. In this capacity he worked with a team responsible for advancing the state of the art in information systems security. He has more than 40 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training.

Dr. Krutz has been an information security consultant at REALTECH Systems Corporation and BAE Systems, an associate director of the Carnegie Mellon Research Institute (CMRI), and a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and director of the CMRI Computer, Automation, and Robotics Group. He is a former lead instructor for the (ISC)² CISSP Common Body of Knowledge review seminars. Dr. Krutz is also a Distinguished Special Lecturer in the Center for Forensic Computer Investigation at the University of New Haven, a part-time instructor in the University of Pittsburgh Department of Electrical and Computer Engineering, and a Registered Professional Engineer.

In addition to being a former lead instructor for the ISC² CBK review seminars and contributing material to the CBK, Dr. Krutz is the author of nine best-selling publications in the area of information systems security, and is a consulting editor for John Wiley and Sons for its information security book series. Dr. Krutz holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering.
viii  About the Authors

RUSSELL DEAN VINES, CISSP, CISM, Security +, CCNA, MCSE, MCNE.
Mr. Vines is president and founder of The RDV Group Inc. (www.rdvgroup.com), a New York-based security consulting services firm. He has been active in the prevention, detection, and remediation of security vulnerabilities for international corporations, including government, finance, and new media organizations, for many years.

Mr. Vines holds high-level certifications in Cisco, 3Com, Ascend, Microsoft, and Novell technologies and is trained in the National Security Agency’s ISSO Information Assessment Methodology. He has headed computer security departments and managed worldwide information systems networks for prominent technology, entertainment, and nonprofit corporations based in New York. He is the author of nine best-selling information system security publications, and is a consulting editor for John Wiley and Sons for its information security book series.

Mr. Vines’s early professional years were illuminated not by the flicker of a computer monitor but by the bright lights of Nevada casino show rooms. After receiving a Down Beat magazine scholarship to Boston’s Berklee College of Music, Mr. Vines performed as a sideman for a variety of well-known entertainers, including George Benson, John Denver, Sammy Davis Jr., and Dean Martin. Mr. Vines composed and arranged hundreds of pieces of jazz and contemporary music, recorded and performed by his own big band and others. He also founded and managed a scholastic music publishing company and worked as an artist-in-residence for the National Endowment for the Arts (NEA) in communities throughout the West. He still performs and teaches music in the New York City area and is a member of the American Federation of Musicians Local 802 and the International Association for Jazz Education. You can find Mr. Vines’s blog at http://rdvgroup.blogspot.com.
Credits

Executive Editor
Carol Long

Development Editor
Rosanne Koneval

Production Editor
William A. Barton

Copy Editor
Publication Services, Inc.

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Joseph B. Wikert

Project Coordinator
Ryan Steffen

Graphics and Production Specialists
Lauren Goddard
Stephanie Jumper
Jennifer Mayberry
Lynsey Osborn

Quality Control Technicians
John Greenough
Jessica Kramer

Media Development Specialists
Angela Denny
Kit Malone
Travis Silvers

Proofreading
Nancy L. Reinhardt

Indexing
Techbooks
Contents

About the Authors vii
Foreword xxiii
Acknowledgments xxv
Introduction xxvii
Part 1 Focused Review of the CISSP Ten Domains 1
Chapter 1 Information Security and Risk Management 3
   Our Approach 4
   Security Management Concepts 5
      System Security Life Cycle 5
      The Three Fundamentals 6
      Other Important Concepts 7
   Objectives of Security Controls 10
   Information Classification Process 12
      Information Classification Objectives 12
      Information Classification Benefits 13
      Information Classification Concepts 13
      Information Classification Roles 16
   Security Policy Implementation 20
      Policies, Standards, Guidelines, and Procedures 20
   Roles and Responsibilities 25
   Risk Management and Assessment 27
      Principles of Risk Management 27
      RM Roles 30
      Overview of Risk Analysis 30
   Security Posture Assessment Methodologies 39
Contents

Security Awareness 42
  Awareness 44
  Training and Education 45
  Assessment Questions 46

Chapter 2 Access Control 55
  Rationale 55
  Controls 56
  Models for Controlling Access 57
    Control Combinations 59
  Access Control Attacks 61
    Denial of Service/Distributed Denial of Service (DoS/DDoS) 61
    Back Door 62
    Spoofing 62
    Man-in-the-Middle 63
    Replay 63
    TCP Hijacking 63
    Social Engineering 64
    Dumpster Diving 64
    Password Guessing 65
    Software Exploitation 65
    Mobile Code 66
    Trojan Horses 66
    Logic Bomb 67
    System Scanning 67
  Penetration Testing 68
  Identification and Authentication 69
    Passwords 70
    Biometrics 72
  Single Sign-On (SSO) 74
    Kerberos 75
    Kerberos Operation 76
    SESAME 79
    KryptoKnight 79
  Access Control Methodologies 79
    Centralized Access Control 80
    Decentralized/Distributed Access Control 81
    Intrusion Detection 86
    Some Access Control Issues 88
  Assessment Questions 89

Chapter 3 Telecommunications and Network Security 95
  The C.I.A. Triad 96
    Confidentiality 96
    Integrity 96
    Availability 97
**Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>98</td>
</tr>
<tr>
<td>The Layered Architecture Concept</td>
<td>98</td>
</tr>
<tr>
<td>Open Systems Interconnect (OSI) Model</td>
<td>99</td>
</tr>
<tr>
<td>Transmission Control Protocol/Internet Protocol (TCP/IP)</td>
<td>103</td>
</tr>
<tr>
<td>LAN Technologies</td>
<td>110</td>
</tr>
<tr>
<td>Ethernet</td>
<td>110</td>
</tr>
<tr>
<td>ARCnet</td>
<td>112</td>
</tr>
<tr>
<td>Token Ring</td>
<td>112</td>
</tr>
<tr>
<td>Fiber Distributed Data Interface (FDDI)</td>
<td>113</td>
</tr>
<tr>
<td>Cabling Types</td>
<td>113</td>
</tr>
<tr>
<td>Coaxial Cable (Coax)</td>
<td>113</td>
</tr>
<tr>
<td>Twisted Pair</td>
<td>114</td>
</tr>
<tr>
<td>Fiber-Optic Cable</td>
<td>116</td>
</tr>
<tr>
<td>Cabling Vulnerabilities</td>
<td>116</td>
</tr>
<tr>
<td>Transmission Types</td>
<td>117</td>
</tr>
<tr>
<td>Network Topologies</td>
<td>118</td>
</tr>
<tr>
<td>Bus</td>
<td>118</td>
</tr>
<tr>
<td>Ring</td>
<td>118</td>
</tr>
<tr>
<td>Star</td>
<td>118</td>
</tr>
<tr>
<td>Tree</td>
<td>120</td>
</tr>
<tr>
<td>Mesh</td>
<td>120</td>
</tr>
<tr>
<td>LAN Transmission Protocols</td>
<td>121</td>
</tr>
<tr>
<td>Carrier-Sense Multiple Access (CSMA)</td>
<td>121</td>
</tr>
<tr>
<td>Polling</td>
<td>122</td>
</tr>
<tr>
<td>Token Passing</td>
<td>122</td>
</tr>
<tr>
<td>Unicast, Multicast, Broadcast</td>
<td>123</td>
</tr>
<tr>
<td>Networking Devices</td>
<td>123</td>
</tr>
<tr>
<td>Hubs and Repeaters</td>
<td>123</td>
</tr>
<tr>
<td>Bridges</td>
<td>124</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>125</td>
</tr>
<tr>
<td>Switches</td>
<td>125</td>
</tr>
<tr>
<td>Transparent Bridging</td>
<td>125</td>
</tr>
<tr>
<td>Routers</td>
<td>126</td>
</tr>
<tr>
<td>VLANs</td>
<td>129</td>
</tr>
<tr>
<td>Gateways</td>
<td>130</td>
</tr>
<tr>
<td>LAN Extenders</td>
<td>130</td>
</tr>
<tr>
<td>Firewall Types</td>
<td>130</td>
</tr>
<tr>
<td>Packet-Filtering Firewalls</td>
<td>131</td>
</tr>
<tr>
<td>Application-Level Firewalls</td>
<td>132</td>
</tr>
<tr>
<td>Circuit-Level Firewalls</td>
<td>133</td>
</tr>
<tr>
<td>Stateful Inspection Firewalls</td>
<td>133</td>
</tr>
<tr>
<td>Firewall Architectures</td>
<td>133</td>
</tr>
<tr>
<td>Packet-Filtering Routers</td>
<td>134</td>
</tr>
<tr>
<td>Screened-Host Firewalls</td>
<td>134</td>
</tr>
<tr>
<td>Dual-Homed Host Firewalls</td>
<td>134</td>
</tr>
<tr>
<td>Screened-Subnet Firewalls</td>
<td>135</td>
</tr>
<tr>
<td>SOCKS</td>
<td>137</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Common Data Network Services</td>
<td>137</td>
</tr>
<tr>
<td>File Transfer Services</td>
<td>138</td>
</tr>
<tr>
<td>SFTP</td>
<td>139</td>
</tr>
<tr>
<td>SSH/SSH-2</td>
<td>139</td>
</tr>
<tr>
<td>TFTP</td>
<td>140</td>
</tr>
<tr>
<td>Data Network Types</td>
<td>140</td>
</tr>
<tr>
<td>Wide Area Networks</td>
<td>141</td>
</tr>
<tr>
<td>Internet</td>
<td>141</td>
</tr>
<tr>
<td>Intranet</td>
<td>142</td>
</tr>
<tr>
<td>Extranet</td>
<td>142</td>
</tr>
<tr>
<td>WAN Technologies</td>
<td>142</td>
</tr>
<tr>
<td>Dedicated Lines</td>
<td>142</td>
</tr>
<tr>
<td>T-carriers</td>
<td>143</td>
</tr>
<tr>
<td>WAN Switching</td>
<td>143</td>
</tr>
<tr>
<td>Circuit-Switched Networks</td>
<td>143</td>
</tr>
<tr>
<td>Packet-Switched Networks</td>
<td>144</td>
</tr>
<tr>
<td>Other WAN Protocols</td>
<td>146</td>
</tr>
<tr>
<td>Common WAN Devices</td>
<td>146</td>
</tr>
<tr>
<td>Network Address Translation (NAT)</td>
<td>147</td>
</tr>
<tr>
<td>Remote Access Technologies</td>
<td>149</td>
</tr>
<tr>
<td>Remote Access Types</td>
<td>149</td>
</tr>
<tr>
<td>Remote Access Security Methods</td>
<td>151</td>
</tr>
<tr>
<td>Virtual Private Networking (VPN)</td>
<td>151</td>
</tr>
<tr>
<td>RADIUS and TACACS</td>
<td>160</td>
</tr>
<tr>
<td>Network Availability</td>
<td>162</td>
</tr>
<tr>
<td>High Availability and Fault Tolerance</td>
<td>162</td>
</tr>
<tr>
<td>Wireless Technologies</td>
<td>164</td>
</tr>
<tr>
<td>IEEE Wireless Standards</td>
<td>164</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>170</td>
</tr>
<tr>
<td>Wireless Application Protocol (WAP)</td>
<td>171</td>
</tr>
<tr>
<td>Wireless Security</td>
<td>174</td>
</tr>
<tr>
<td>Wireless Transport Layer Security Protocol</td>
<td>174</td>
</tr>
<tr>
<td>WEP Encryption</td>
<td>175</td>
</tr>
<tr>
<td>Wireless Vulnerabilities</td>
<td>175</td>
</tr>
<tr>
<td>Intrusion Detection and Response</td>
<td>183</td>
</tr>
<tr>
<td>Types of Intrusion Detection Systems</td>
<td>183</td>
</tr>
<tr>
<td>IDS Approaches</td>
<td>184</td>
</tr>
<tr>
<td>Honey Pots</td>
<td>186</td>
</tr>
<tr>
<td>Computer Incident Response Team</td>
<td>187</td>
</tr>
<tr>
<td>IDS and a Layered Security Approach</td>
<td>188</td>
</tr>
<tr>
<td>IDS and Switches</td>
<td>188</td>
</tr>
<tr>
<td>IDS Performance</td>
<td>190</td>
</tr>
<tr>
<td>Network Attacks and Abuses</td>
<td>190</td>
</tr>
<tr>
<td>Logon Abuse</td>
<td>190</td>
</tr>
<tr>
<td>Inappropriate System Use</td>
<td>190</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>191</td>
</tr>
<tr>
<td>Network Intrusion</td>
<td>191</td>
</tr>
</tbody>
</table>
Denial of Service (DoS) Attacks 192
Session Hijacking Attacks 192
Fragmentation Attacks 193
Dial-Up Attacks 193
Probing and Scanning 194
Vulnerability Scanning 194
Port Scanning 195
Issues with Vulnerability Scanning 201
Malicious Code 202
Viruses 202
Spyware 204
Trojan Horses 210
Remote Access Trojans (RATs) 211
Logic Bombs 212
Worms 212
Malicious Code Prevention 212
Web Security 214
Phishing 214
Browser Hijacking 214
SSL/TLS 215
S-HTTP 217
Instant Messaging Security 217
8.3 Naming Conventions 221
Assessment Questions 222

Chapter 4 Cryptography 233
Introduction 233
Definitions 234
Background 238
Cryptographic Technologies 241
Classical Ciphers 241
Substitution 241
Transposition (Permutation) 244
Vernam Cipher (One-Time Pad) 244
Book or Running-Key Cipher 245
Codes 245
Steganography 245
Secret-Key Cryptography (Symmetric-Key) 246
Data Encryption Standard (DES) 247
Triple DES 251
The Advanced Encryption Standard (AES) 252
The Rijndael Block Cipher 253
The Twofish Algorithm 254
The IDEA Cipher 255
RC5/RC6 255
Public-Key (Asymmetric) Cryptosystems 255
One-Way Functions 256
Public-Key Algorithms 256
# Contents

The Software Life Cycle Development Process 399
   The Waterfall Model 400
   The Spiral Model 403
   Cost Estimation Models 406
   Information Security and the Life Cycle Model 407
   Testing Issues 408
   The Software Maintenance Phase and the Change Control Process 408
   Configuration Management 409
The Software Capability Maturity Model (CMM) 410
Agile Methodology 412
Object-Oriented Systems 413
Artificial Intelligence Systems 417
   Expert Systems 417
   Neural Networks 419
   Genetic Algorithms 421
   Knowledge Management 421
Database Systems 421
   Database Security Issues 422
   Data Warehouse and Data Mining 422
Data Dictionaries 423
Application Controls 423
   Distributed Systems 425
   Centralized Architecture 426
   Real-Time Systems 426
Assessment Questions 427

## Chapter 8 Business Continuity Planning and Disaster Recovery Planning 433

Business Continuity Planning 435
   Continuity Disruptive Events 436
   The Four Prime Elements of BCP 437
Disaster Recovery Planning (DRP) 446
   Goals and Objectives of DRP 446
   The Disaster Recovery Planning Process 447
   Testing the Disaster Recovery Plan 455
   Disaster Recovery Procedures 459
   Other Recovery Issues 461
Assessment Questions 464

## Chapter 9 Legal, Regulations, Compliance, and Investigations 473

Types of Computer Crime 473
Examples of Computer Crime 475
Law 477
   Example: The United States 477
   Common Law System Categories 478
   Computer Security, Privacy, and Crime Laws 489
Investigation
  Computer Investigation Issues 496
  Export Issues and Technology 502
Liability 502
Ethics 504
  (ISC)2 Code of Ethics 506
  The Computer Ethics Institute’s Ten Commandments of Computer Ethics 506
  The Internet Architecture Board (IAB) Ethics and the Internet (RFC 1087) 507
  The U.S. Department of Health and Human Services Code of Fair Information Practices 507
  The Organization for Economic Cooperation and Development (OECD) 508
Assessment Questions 510

Chapter 10 Physical (Environmental) Security 517
  Threats to Physical Security 518
  Controls for Physical Security 520
    Administrative Controls 520
    Environmental and Life Safety Controls 524
    Physical and Technical Controls 534
Assessment Questions 550

Part 2 The Certification and Accreditation Professional (CAP) Credential 557

Chapter 11 Understanding Certification and Accreditation 559
  System Authorization 559
    A Select History of Systems Authorization 560
    More and More Standards 572
  What Is Certification and Accreditation? 572
    NIST C&A Documents 573
    C&A Roles and Responsibilities 573
    C&A Phases 577
    DIACAP Phases 578
Assessment Questions 580

Chapter 12 Initiation of the System Authorization Process 585
  Security Categorization 586
    Identification of Information Types 588
    Potential Harmful Impact Levels 589
    Assignment of Impact Level Scores 590
    Assignment of System Impact Level 592
  Initial Risk Estimation 593
    Threat-Source Identification 594
    Threat Likelihood of Occurrence 597
    Analyzing for Vulnerabilities 597
  System Accreditation Boundary 601
  Legal and Regulatory Requirements 603
## Contents

Selection of Security Controls ................................. 603
  The Control Section ........................................... 606
  The Supplemental Guidance Section .......................... 606
  The Control Enhancements Section ............................ 606
  Assurance ....................................................... 607
  Common and System-Specific Security Controls ............. 608
  Security Controls and the Management of Organizational Risk 608
Documenting Security Controls in the System Security Plan ...... 610
Assessment Questions .............................................. 613

### Chapter 13 The Certification Phase .......................... 621

Security Control Assessment .................................... 622
  Prepare for the Assessment ................................... 622
  Conduct the Security Assessment ............................ 624
  Prepare the Security Assessment Report ..................... 624
Security Certification Documentation .......................... 625
  Provide the Findings and Recommendations .................. 625
  Update the System Security Plan ............................ 625
  Prepare the Plan of Action .................................... 626
  Assemble the Accreditation Package .......................... 626
DITSCAP Certification Phases .................................... 627
  Phase 1: Definition ............................................ 627
  SSAA Outline .................................................. 630
  SSAA Additional Material ...................................... 632
  The Requirements Traceability Matrix (RTM) .................. 633
  Phase 2: Verification .......................................... 635
  Key DITSCAP Roles ............................................. 638
DIACAP Certification Phases ...................................... 639
End of the Certification Phase .................................... 640
Assessment Questions .............................................. 641

### Chapter 14 The Accreditation Phase ......................... 645

Security Accreditation Decision ............................... 646
  Final Risk Assessment ........................................ 646
  Accreditation Decision ....................................... 647
Security Accreditation Documentation .......................... 648
  Accreditation Package Transmission ........................ 648
  System Security Plan Update .................................. 649
DITSCAP Accreditation Phases .................................... 649
  Phase 3: Validation ............................................ 649
  Phase 4: Post Accreditation ................................... 653
DIACAP Accreditation Phases ...................................... 656
End of the Accreditation Phase .................................... 657
Assessment Questions .............................................. 658
## Contents

<table>
<thead>
<tr>
<th>Chapter 15</th>
<th>Continuous Monitoring Process</th>
<th>663</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Continuous Monitoring</td>
<td>664</td>
</tr>
<tr>
<td></td>
<td>Monitoring Security Controls</td>
<td>665</td>
</tr>
<tr>
<td></td>
<td>Configuration Management and Control</td>
<td>669</td>
</tr>
<tr>
<td></td>
<td>Environment Monitoring</td>
<td>670</td>
</tr>
<tr>
<td></td>
<td>Documentation and Reporting</td>
<td>671</td>
</tr>
<tr>
<td></td>
<td>Assessment Questions</td>
<td>673</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Answers to Assessment Questions</td>
<td>681</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Glossary of Terms and Acronyms</td>
<td>881</td>
</tr>
<tr>
<td>Appendix C</td>
<td>The Information System Security Architecture Professional (ISSAP) Certification</td>
<td>945</td>
</tr>
<tr>
<td>Appendix D</td>
<td>The Information System Security Engineering Professional (ISSEP) Certification</td>
<td>951</td>
</tr>
<tr>
<td>Appendix E</td>
<td>The Information System Security Management Professional (ISSMP) Certification</td>
<td>1039</td>
</tr>
<tr>
<td>Appendix F</td>
<td>Security Control Catalog</td>
<td>1075</td>
</tr>
<tr>
<td>Appendix G</td>
<td>Control Baselines</td>
<td>1185</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>1193</td>
</tr>
</tbody>
</table>
In the years since its first edition, the CISSP Prep Guide has become a most valuable resource for people interested in pursuing the CISSP credential. It also has that rare quality of having withstood the test of time and continues to appear on bookshelves for reference purposes even for those who have earned the CISSP. We are happy and proud to be associated with the CISSP Prep Guide from the start.

We have been involved with dozens of situations in which the CISSP skill set has been at the core of what is needed in “security” events. The holistic body of knowledge mastered by a CISSP is designed to ensure that you will not suffer from a focus that is too narrow, yet it is oriented to detail in the critical areas. Today more than ever, IT professionals need credentials and expertise with the sophisticated tools that can be used to scour their companies’ computers for signs of covert network connections, evidence showing unauthorized insider access to system resources, remnants from Web-based email sessions, or files that may have been used in unauthorized ways.

Many security issues today draw heavily from legal considerations that have to be taken into account before a company will make a decision. It has been our experience that advice and guidance from a person having the CISSP is reassuring because the credential serves as a badge of credibility in reassuring lawyers who advise companies. Many of the professionals we work with in industry and in government, including the FBI, have either obtained or are pursuing their CISSP.

As with other professional services, the CISSP makes his or her company stronger by the actions he or she takes day-to-day. However, sometimes events can escalate is some situations where there are indications of intentional
wrongdoing. Those situations, when they arise, almost always cause legal options to be explored. The CISSP brings great credibility to those discussions.

The actions taken each day by CISSPs to maintain and keep current the security of the systems they oversee are vitally important and will help avoid ever having to confront such a disruptive event. We encourage you to draw from the CISSP and CAP Prep Guide as you prepare for the CISSP test, and thereafter as you improve the security of the organizations you serve.

Edward M. Stroz is Managing Partner of Stroz Friedberg, LLC, a consulting and professional services firm dedicated to expertise in computer forensics, computer crimes investigations, and security. Before founding the firm in 2000, he spent 16 years with the FBI, where he formed and supervised the computer crime squad in the New York field office.

Aaron Stanley, CISSP, is Director of Information Technology at Stroz Friedberg, LLC. An accomplished investigator, security consultant, and IT manager, he led many of the initiatives discussed in the case study above.
I want to thank my wife, Hilda, for her continuous support and guidance during this project.

—R.L.K.

I would like to thank Dr. David Altcheck and Dr. Lawrence Levin, who have brought the joy of mobility back into my life. And to all my friends, and especially my wife, Elzy, for their continual support.

—R.D.V.

Both authors would like to express a special thanks to Carol Long and Rosanne Koneval of John Wiley and Sons for their support and assistance in developing this text.
The need to protect information resources has produced a demand for information systems security professionals. Along with this demand came a need to ensure that these professionals possess the knowledge to perform the required job functions. To address this need, the Certified Information Systems Security Professional (CISSP) certification emerged. This certification guarantees to all parties that the certified individual meets the standard criteria of knowledge and continues to upgrade that knowledge in the field of information systems security. The CISSP initiative also serves to enhance the recognition and reputation of the field of information security.

Realizing the importance of certification and accreditation to the global security effort, the U.S. Department of State’s Office of Information Assurance and (ISC)² have collaborated to develop a credential for the Certification and Accreditation Professional (CAP). The CAP credential is an objective measure of the knowledge, skills and abilities required for personnel involved in the Certification and Accreditation process. Specifically, the credential applies to professionals responsible for formalizing processes used to assess risk and establish security requirements, as well as ensure information systems possess security commensurate with the level of exposure to potential risk. CAP is a fully independent credential, meaning that it is on the same level as the CISSP and SSCP credentials. It does not require CISSP certification as the advanced concentrations do (ISSAP, ISSEP, and ISSMP). The reader for the CAP portion of the book, as defined by (ISC)², should have some experience in one or more of a number of areas, including:

- IT security
- Information assurance
For the CISSP who wishes to concentrate in information systems security for U.S. federal information systems, the CISSP Information System Security Engineering Professional (ISSEP®) concentration certification has been established. This certification is particularly relevant for efforts in conjunction with the National Security Agency (NSA) and with other U.S. government agencies. The ISSEP concentration address four additional areas related to U.S. Government information assurance, particularly NSA information assurance. These four areas are:

- Systems Security Engineering
- Certification and Accreditation
- Technical Management
- U.S. Government Information Assurance Regulations

The ISSAP Certification is defined by (ISC)^2 as the CISSP concentration area that is designed to denote competence and expertise in information security architecture, telecommunications, preservation of business operations, and related security issues. To qualify for and obtain the ISSAP certification, the candidate must possess the CISSP credential, sit for and pass the ISSAP examination, and maintain the ISSAP credential in good standing.

The ISSMP Certification is defined by (ISC)^2 as the CISSP concentration area that is designed to denote competence and expertise in information security management. The ISSMP certification and examination cover enterprise security management, enterprisewide systems development, compliance of operations security, business continuity planning (BCP), disaster recovery planning (DRP), continuity of operations planning (COOP), and law, investigation, forensics, and ethics.

The material relevant to the ISSEP, ISSAP, and ISSMP certifications are presented in Appendices C, D, and E of this text.

The primary audience for the material in this book includes:

- Professionals working in the fields of information technology or information system security
- Computer forensics professionals