WILEY

TIMELY. PRACTICAL. RELIABLE.

CISSP® Practice

2,250 Questions, Answers, and Explanations for Passing the Test

S. Rao Vallabhaneni

CISSP® Practice

CISSP® Practice

2,250 QUESTIONS, ANSWERS, AND EXPLANATIONS FOR PASSING THE TEST

S. Rao Vallabhaneni

John Wiley & Sons, Inc.

CISSP® Practice: 2,250 Questions, Answers, and Explanations for Passing the Test

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-118-10594-8
ISBN: 978-1-118-17612-2 (ebk)
ISBN: 978-1-118-17613-9 (ebk)
ISBN: 978-1-118-17614-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2011936911

This book is dedicated to my parents who taught me from the beginning that education is the only thing that endures.

ABOUT THE AUTHOR

S. RAO VALLABHANENI is an educator, author, publisher, consultant, and practitioner in the business field, with more than 30 years of management and teaching experience in manufacturing, finance, accounting, auditing, and information technology. He has authored more than 60 books, mostly study guides to help students prepare for for several professional certification exams, in various business functions. He earned four master's degrees in management, accounting, industrial engineering, and chemical engineering, and holds 24 professional certifications in various business disciplines. He is a graduate of the Advanced Management Development Program at the University of Chicago's Graduate School of Business.

He is the recipient of the 2004 Joseph J. Wasserman Memorial Award for the distinguished contribution to the Information Systems Audit field, conferred by the New York Chapter of the Information Systems Audit and Control Association (ISACA). He is the first independent author and publisher in the CISSP Exam market to develop a comprehensive two-volume (Practice and Theory) reviewing products to help students prepare for the CISSP Exam in 2000. In addition to teaching undergraduate and graduate courses in business schools, he taught the Certified Information Systems Auditor (CISA) Exam and the Certified Internal Auditor (CIA) Exam review courses to prepare for these exams.

ABOUT THE TECHNICAL EDITOR

RONALD L. KRUTZ is a senior information system security consultant. He has over 30 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training. He holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering and is the author of best-selling texts in the area of information system security. Dr. Krutz is a Certified Information Systems Security Professional (CISSP) and Information Systems Security Engineering Professional (ISSEP).

He coauthored the *CISSP Prep Guide* for John Wiley & Sons and is coauthor of the Wiley *Advanced CISSP Prep Guide*; *CISSP Prep Guide, Gold Edition*; *Security +Certification Guide*; *CISM Prep Guide*; *CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP*; *Network Security Bible*, *CISSP and CAP Prep Guide*, *Platinum Edition: Mastering CISSP and CAP*; *Certified Ethical Hacker (CEH) Prep Guide*; *Certified Secure Software Lifecycle Prep Guide*, *Cloud Security,* and *Web Commerce Security*.

He is also the author of *Securing SCADA Systems* and of three textbooks in the areas of microcomputer system design, computer interfacing, and computer architecture. Dr. Krutz has seven patents in the area of digital systems and has published over 40 technical papers. Dr. Krutz is a Registered Professional Engineer in Pennsylvania.

CREDITS

EXECUTIVE EDITOR
Carol Long

PROJECT EDITOR
Maureen Spears

TECHNICAL EDITOR
Ronald Krutz

SENIOR PRODUCTION EDITOR
Debra Banninger

COPY EDITOR
Apostrophe Editing Services

EDITORIAL MANAGER
Mary Beth Wakefield

FREELANCER EDITORIAL MANAGER
Rosemarie Graham

MARKETING MANAGER
Ashley Zurcher

PRODUCTION MANAGER
Tim Tate

VICE PRESIDENT AND EXECUTIVE GROUP PUBLISHER
Richard Swadley

VICE PRESIDENT AND EXECUTIVE PUBLISHER
Neil Edde

ASSOCIATE PUBLISHER
Jim Minatel

PROJECT COORDINATOR, COVER
Katie Crocker

COMPOSITOR
JoAnn Kolonick,
Happenstance Type-O-Rama

PROOFREADER
Kristy Eldredge,
Word One

INDEXER
Robert Swanson

COVER IMAGE
© Peter Nguyen / iStockPhoto

COVER DESIGNER
Ryan Sneed

ACKNOWLEDGMENTS

I WANT TO THANK the following organizations and institutions for enabling me to use their publications and reports. They were valuable and authoritative resources for developing the practice questions, answers, and explanations.

- ISC2, Inc., for the use of its Common Body of Knowledge described in the "CISSP Candidate Information Bulletin," January 1, 2012.
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Gaithersburg, Maryland, for the use of various IT-related publications (FIPS, NISTIR, SP 500 series, SP 800 series).
- National Communications System (NCS) and the U.S. Department of Defense (DOD) for their selected IT-related publications.
- U.S. Government Accountability Office (GAO), formerly known as General Accounting Office, Washington, DC, for various IT-related reports and staff studies.
- Office of Technology Assessment (OTA), U.S. Congress, Washington, DC, for various publications in IT security and privacy in network technology.
- Office of Management and Budget (OMB), Washington, DC, for selected publications in IT security and privacy.
- Federal Trade Commission (FTC), Washington, DC, at `www.ftc.gov`.
- Chief Information Officer (CIO) council, Washington, DC at `www.cio.gov`.
- Information Assurance Technical Framework (IATF), Release 3.1, National Security Agency (NSA), Fort Meade, Maryland, September 2002.
- Security Technical Implementation Guides (STIGs) by Defense Information Systems Agency (DISA) developed for the U.S. Department of Defense (DOD).

I want to thank the following individuals for helping me to improve the content, quality, and completeness of this book:

- Dean Bushmiller, of Austin, Texas, for grouping the author's questions and making them into scenario-based questions and answers. Dean teaches the CISSP Exam and CISM Exam review classes to prepare for the exams.
- Carol A. Long, executive acquisitions editor at Wiley Publishing, Inc., for publishing this book.
- Ronald Krutz (technical editor), Apostrophe Editing Services (copy editor) and all the people at Wiley who made this book possible.

CISSP PRACTICE

PREFACE *xvii*

DOMAIN 1: ACCESS CONTROL **1**

Scenario-Based Questions, Answers, and Explanations. 124
Sources and References 128

DOMAIN 2: TELECOMMUNICATIONS AND NETWORK SECURITY **129**

Traditional Questions, Answers, and Explanations 129
Scenario-Based Questions, Answers, and Explanations. 263
Sources and References 266

DOMAIN 3: INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT **269**

Traditional Questions, Answers, and Explanations 269
Scenario-Based Questions, Answers, and Explanations. 346
Sources and References 350

DOMAIN 4: SOFTWARE DEVELOPMENT SECURITY **351**

Traditional Questions, Answers, and Explanations 351
Scenario-Based Questions, Answers, and Explanations. 434
Sources and References 437

DOMAIN 5: CRYPTOGRAPHY **439**

Traditional Questions, Answers, and Explanations 439
Scenario-Based Questions, Answers, and Explanations. 523
Sources and References 525

DOMAIN 6: SECURITY ARCHITECTURE AND DESIGN **527**

Traditional Questions, Answers, and Explanations 527
Scenario-Based Questions, Answers, and Explanations. 607
Sources and References 612

DOMAIN 7: SECURITY OPERATIONS 613

Traditional Questions, Answers, and Explanations 613
Scenario-Based Questions, Answers, and Explanations. 694
Sources and References 698

DOMAIN 8: BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING 699

Traditional Questions, Answers, and Explanations 699
Scenario-Based Questions, Answers, and Explanations 740
Sources and References 742

DOMAIN 9: LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE 743

Traditional Questions, Answers, and Explanations 743
Scenario-Based Questions, Answers, and Explanations. 823
Sources and References 825

DOMAIN 10: PHYSICAL AND ENVIRONMENTAL SECURITY 827

Traditional Questions, Answers, and Explanations 827
Scenario-Based Questions, Answers, and Explanations. 863
Sources and References 866

APPENDIX A: CISSP GLOSSARY 2012 867

APPENDIX B: CISSP ACRONYMS AND ABBREVIATIONS 2012 1057

INDEX 1083

PREFACE

The purpose of *CISSP Practice: 2,250 Questions, Answers, and Explanations for Passing the Test* is to help the Certified Information Systems Security Professional (CISSP) examination candidates prepare for the exam by studying and practicing the sample test questions with the goal to succeed on the exam.

A total of 2,250 traditional multiple-choice (M/C) questions, answers, and explanations are presented in this book. In addition, a total of 82 scenario-based M/C questions, answers, and explanations are taken from the traditional 2,250 questions and grouped into the scenario-based format to give a f avor to the scenario questions. Traditional questions contain one stem followed by one question set with four choices of a., b., c., and d., and scenario questions contain one stem followed by several question sets with four choices of a., b., c., and d. The scenario-based questions can focus on more than one domain to test the comprehensive application of the subject matter in an integrated manner whereas the traditional questions focus on a single domain.

These 2,250 sample test practice questions are not duplicate questions and are not taken from the ISC2 or from anywhere else. The author developed these unique M/C questions for each domain based on the current CISSP Exam content specifications (see the "Description of the CISSP Examination" later in this preface). Each unique and insightful question focuses on a specific and necessary depth and breadth of the subject matter covered in the CISSP Exam.

The author sincerely believes that the more questions you practice, the better prepared you are to take the CISSP Exam with greater confidence because the real exam includes 250 questions. The total number of 2,250 questions represents nine times the number of questions tested on the exam, thus providing a great value to the CISSP Exam candidate. This value is in the form of increasing the chances to pass the CISSP Exam.

Because ISC2 did not publish the percentage-weights for ten domains, the author has assigned the following percentage-weights for each domain (for example, Domain 1 = 15%) based on what he thinks is important to the CISSP Exam candidate. These assigned weights are based on the author's assumption that all the ten domains cannot receive equal weight in the exam due to the differences in relative importance of these domains. These weights are assigned as a systematic way to distribute the 2,250 questions among the ten domains, as follows:

- Domain 1: Access Control (**15%**)
- Domain 2: Telecommunications and Network Security (**15%**)
- Domain 3: Information Security Governance and Risk Management (**10%**)
- Domain 4: Software Development Security (**10%**)
- Domain 5: Cryptography (**10%**)
- Domain 6: Security Architecture and Design (**10%**)
- Domain 7: Security Operations (**10%**)

- Domain 8: Business Continuity and Disaster Recovery Planning (**5%**)
- Domain 9: Legal, Regulations, Investigations, and Compliance (**10%**)
- Domain 10: Physical and Environmental Security (**5%**)

The following table presents the number of traditional questions and scenario questions for each of the ten domains.

DOMAIN	TRADITIONAL QUESTIONS	SCENARIO QUESTIONS
1	338 (2,250 x 15%)	9
2	338	7
3	225	9
4	225	11
5	225	7
6	225	12
7	225	8
8	112	7
9	225	5
10	112	7
Totals	**2,250**	**82**

The real CISSP Exam consists of 250 M/C questions with four choices of a., b., c., and d. for each question. There can be some scenario-based questions in addition to most of traditional questions. Regardless of the type of questions on the exam, there is only one correct answer (choice). You must complete the entire CISSP Exam in one six-hour session. The scope of the CISSP Exam consists of the subject matter covered in ten domains of this book, which is in accordance with the description of the CISSP Exam (content specifications) as defined in the ISC2's "CISSP Candidate Information Bulletin" with an **effective date of January 1, 2012.** Note that these practice questions are also good for the CISSP Exam with an effective date of January 1, 2009 because we accommodated both effective dates (January 2009 and January 2012) due to their minor differences in the content specifications.

With no bias intended and for the sake of simplicity, the pronoun "he" has been used throughout the book rather than "he/she" or "she."

—S. Rao Vallabhaneni
Chicago, Illinois
August 2011

HOW TO STUDY FOR THE CISSP EXAM

To study for the CISSP Exam, follow these guidelines:

- Read the official description of the CISSP Exam at the end of this section.
- Read the glossary terms and acronyms found in Appendixes A and B at the back of this book to become familiar with the technical terms and acronyms.
- Take the sample practice tests for each of the ten domains.
- If you score less than 75 percent for each domain, study the glossary terms again until you master the subject matter or score higher than 75 percent.
- Complete the scenario-based practice questions to integrate your learning and thought processes.

The types of questions a candidate can expect to see on the CISSP Exam are mostly objective and traditional multiple-choice questions and some scenario-based multiple-choice questions with only one choice as the correct answer. Answering these multiple-choice questions requires a significant amount of practice and effort.

The following tips and techniques are helpful for answering the multiple-choice questions:

- Stay with your first impression of the correct choice.
- Know the subject area or topic. Don't read too much into the question.
- Remember that all questions are independent of specific countries, products, practices, vendors, hardware, software, or industries.
- Read the last sentence of the question first, followed by all the choicesthen read the body of the question. Underline or circle the key words.
- Read the question twice (or read the underlined or circled key words twice) and watch for tip-off words such as *not, except, all, every, always, never, least,* or *most* that denote absolute conditions.
- Don't project the question into your own organizational environment, practices, policies, procedures, standards, and guidelines.
- Try to eliminate wrong choices quickly by striking or drawing a line through the choices or by using other ways convenient to you.
- When you are left with two probable choices after the process of elimination, take a big picture approach. For example, if choices a. and d. remain and choice d. could be a part of choice a., then select choice a. However, if choice d. could be a more complete answer, then select choice d.
- Don't spend too much time on one question. If you are not sure of an answer, move on and come back to it if time permits. The last resort is to guess the answer. There is no penalty for guessing a wrong answer.

- Transfer all questions to the answer sheet either after each question is answered individually or in small groups of 10 or 15 questions. Allocate sufficient time for this task because it is important. Mark the right answer in the correct circle on the answer sheet.

Remember that success on the exam depends on your education and experience, time-management skills, preparation effort and time, memory recall of the subject matter, state of mind, and decision-making skills.

DESCRIPTION OF THE CISSP EXAMINATION

The following is the official description of the Certified Information System Security Professional (CISSP) Examination content specifications as defined in the ISC2's "CISSP Candidate Information Bulletin" with an **effective date of January 1, 2012.** The scope of the CISSP Exam consists of the following subject matter (content specifications) covered in the ten domains.

DOMAIN 1: ACCESS CONTROL

Overview

Access control domain covers any mechanism by which a system grants or revokes the right to access data or perform some action. The access control mechanism controls various operations a user may or may not perform.

Access controls systems include

- File permissions such as create, read, edit, or delete on a file server
- Program permissions such as the right to execute a program on an application server
- Data rights such as the right to retrieve or update information in a database

The candidate should fully understand access control concepts, methodologies, and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques and detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Key Areas of Knowledge

- Control access by applying the following concepts/methodologies/techniques.
  1. Policies
  2. Types of controls such as preventive, detective, and corrective
  3. Techniques such as nondiscretionary, discretionary, and mandatory
  4. Identification and authentication
  5. Decentralized/distributed access control techniques

6. Authorization mechanisms
7. Logging and monitoring

- Understand access control attacks.
  1. Threat modeling
  2. Asset valuation
  3. Vulnerability analysis
  4. Access aggregation
- Assess effectiveness of access controls.
  1. User entitlement
  2. Access review and audit
- Identity and access provisioning life cycle such as provisioning, review, and revocation.

DOMAIN 2: TELECOMMUNICATIONS AND NETWORK SECURITY

Overview

The telecommunications and network security domain encompasses the structures, techniques, transport protocols, and security measures used to provide integrity, availability, confidentiality, and authentication for transmissions over private and public communications networks and media.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local-area and wide-area networks, remote access; Internet/intranet/extranet configurations, and other network equipment (such as switches, bridges, and routers), protocols (such as TCP/IP); VPNs and, techniques (such as the correct use and placement of firewalls and IDS) for preventing and detecting network based attacks.

Key Areas of Knowledge

- Understand secure network architecture and design such as IP and non-IP protocols, and segmentation.
  1. OSI and TCP/IP models
  2. IP networking
  3. Implications of multi-layer protocols
- Secure network components.
  1. Hardware such as modems, switches, routers, and wireless access points
  2. Transmission media such as wired, wireless, and fiber

3. Network access control devices such as firewalls and proxies
4. End-point security

- Establish secure communication channels such as VPN, TLS/SSL, and VLAN.
  1. Voice such as POTS, PBX, and VoIP
  2. Multimedia collaboration such as remote meeting technology and instant messaging
  3. Remote access such as screen scraper, virtual application/desktop, and telecommuting
  4. Data communications
- Understand network attacks such as DDoS and spoofing.

DOMAIN 3: INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT

Overview

Information security governance and risk management domain entails the identification of an organization's information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, and roles and responsibilities of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics, and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary, and private information; third party management and service level agreements related to information security; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

Key Areas of Knowledge

- Understand and align security function to goals, mission, and objectives of the organization.
- Understand and apply security governance.
  1. Organizational processes such as acquisitions, divestitures, and governance committees
  2. Security roles and responsibilities
  3. Legislative and regulatory compliance
  4. Privacy requirements compliance

5. Control frameworks
6. Due care
7. Due diligence

- Understand and apply concepts of confidentiality, integrity, and availability.
- Develop and implement security policy.
  1. Security policies
  2. Standards/baselines
  3. Procedures
  4. Guidelines
  5. Documentation
- Manage the information life cycle such as classification, categorization, and ownership.
- Manage third-party governance such as onsite assessment, document exchange and review, and process/poly review.
- Understand and apply risk management concepts.
  1. Identify threats and vulnerabilities
  2. Risk assessments/analysis such as qualitative, quantitative, and hybrid
  3. Risk assignment/acceptance
  4. Countermeasure selection
  5. Tangible and intangible asset valuation
- Manage personnel security.
  1. Employment candidate screening such as reference checks, education, and verification
  2. Employment agreements and policies
  3. Employee termination processes
  4. Vendor, consultant, and contractor controls
- Develop and manage security education, training, and awareness.
- Manage the security function.
  1. Budget
  2. Metrics
  3. Resources
  4. Develop and implement information security strategies
  5. Assess the completeness and effectiveness of the security program

DOMAIN 4: SOFTWARE DEVELOPMENT SECURITY

Overview

Software development security domain refers to the controls that are included within systems and applications software and the steps used in their development. Software refers to system software (operating systems) and application programs (agents, applets, software, databases, data warehouses, and knowledge-based systems). These applications may be used in distributed or centralized environments.

The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.

Key Areas of Knowledge

- Understand and apply security in the software development life cycle.
  1. Development life cycle
  2. Maturity models
  3. Operation and maintenance
  4. Change management
- Understand the environment and security controls.
  1. Security of the software environment
  2. Security issues of programming languages
  3. Security issues in source code such as buffer overf ow, escalation of privilege, and backdoor
  4. Configuration management
- Assess the effectiveness of software security.
  1. Certification and accreditation such as system authorization
  2. Auditing and logging
  3. Risk analysis and mitigation

DOMAIN 5: CRYPTOGRAPHY

Overview

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The candidate is expected to know the basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; the applications, construction, use of digital signatures to provide authenticity of electronic transactions, and nonrepudiation of the parties involved; and the organization and management of the public key infrastructures (PKIs) and digital certificates distribution and management.

Key Areas of Knowledge

- Understand the application and use of cryptography:
  1. Data at rest (e.g., Hard drive)
  2. Data in transit (e.g., On the wire)
- Understand the cryptographic life cycle such as cryptographic limitations, algorithm/protocol governance.
- Understand encryption concepts.
  1. Foundational concepts
  2. Symmetric cryptography
  3. Asymmetric cryptography
  4. Hybrid cryptography
  5. Message digests
  6. Hashing

- Understand key management processes.
  1. Creation/distribution
  2. Storage/destruction
  3. Recovery
  4. Key escrow
- Understand digital signatures.
- Understand nonrepudiation.
- Understand methods of cryptanalytic attacks.
  1. Chosen plaintext
  2. Social engineering for key discovery
  3. Brute force such as rainbow tables, specialized/scalable architecture
  4. Ciphertext only
  5. Known plaintext
  6. Frequency analysis
  7. Chosen ciphertext
  8. Implementation attacks
- Use cryptography to maintain network security.
- Use cryptography to maintain application security.
- Understand public key infrastructure (PKI).
- Understand certificate-related issues.
- Understand information-hiding alternatives such as steganography and watermarking.

DOMAIN 6: SECURITY ARCHITECTURE AND DESIGN

Overview

The security architecture and design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

Information security architecture and design covers the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that these practices and processes align with the organization's core goals and strategic direction.

The candidate is expected to understand security models in terms of confidentiality, integrity, information f ow; system models in terms of the Common Criteria (CC); technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

Key Areas of Knowledge

- Understand the fundamental concepts of security models (e.g., confidentiality, integrity, and multilevel models).
- Understand the components of information systems security evaluation models.
  1. Product evaluation models such as Common Criteria
  2. Industry and international security implementation guidelines such as PCI-DSS and ISO
- Understand security capabilities of information systems (e.g., memory protection, virtualization, and trusted platform module).
- Understand the vulnerabilities of security architectures.
  1. Systems such as covert channels, state attacks, and emanations
  2. Technology and process integration such as single point of failure and service-oriented architecture (SOA)
- Understand software and system vulnerabilities and threats.
  1. Web-based vulnerabilities/threats such as XML, SAML, and OWASP
  2. Client-based vulnerabilities/threats such as applets
  3. Server-based vulnerabilities/threats such as data f ow control
  4. Database security such as inference, aggregation, data mining, and data warehousing
  5. Distributed systems such as cloud computing, grid computing, and peer-to-peer computing
- Understand countermeasure principles such as defense-in-depth.

DOMAIN 7: SECURITY OPERATIONS

Overview

Security operations domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. It includes the definition of the controls over hardware, media, and **the** operators with access privileges to any of these resources. Auditing and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate is expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

Key Areas of Knowledge

- Understand security operations concepts.
  1. Need-to-know/least privilege
  2. Separation of duties and responsibilities
  3. Monitor special privileges (e.g., operators and administrators)
  4. Job rotation
  5. Marking, handling, storing, and destroying of sensitive information
  6. Record retention
- Employ resource protection.
  1. Media management
  2. Asset management (e.g., equipment life cycle and software licensing)
- Manage incident response.
  1. Detection
  2. Response
  3. Reporting
  4. Recovery
  5. Remediation and review (e.g., root cause analysis)
- Implement preventative measures against attacks (e.g., malicious code, zero-day exploit, and denial-of-service).
- Implement and support patch and vulnerability management.
- Understand change and configuration management (e.g., versioning and base lining).
- Understand system resilience and fault tolerance requirements.

DOMAIN 8: BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Overview

The business continuity planning (BCP) and disaster recovery planning (DRP) domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and