



CCSP[®]

Certified Cloud Security Professional

An (ISC)² Certification

Official Study Guide

Second Edition

Ben Malisow, CCSP, CISSP

Covers 100% of exam objectives, including Cloud Data Security, Cloud Application Security, Cloud Security Operations, Cloud Platform and Infrastructure Security, and much more...

Includes interactive online learning environment and study tools with:

- Two complete custom practice exams
- Over 100 electronic flashcards
- Searchable glossary of terms



(ISC)²® CCSP[®]
Certified Cloud Security
Professional
Official Study Guide



(ISC)²® CCSP[®]
Certified Cloud Security
Professional
Official Study Guide



Ben Malisow

Copyright © 2020 by John Wiley & Sons, Inc.

Published simultaneously in Canada

ISBN: 978-1-119-60337-5

ISBN: 978-1-119-60338-2 (ebk.)

ISBN: 978-1-119-60336-8 (ebk.)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019954578

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. (ISC)2 and CCSP are registered trademarks or certification marks of the International Information Systems Security Certification Consortium, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Acknowledgments

The author would like to thank (ISC)² for making this work possible, and the sublime publishing and editing team at Sybex, including Jim Minatel, Kelly Talbot, Katie Wisor, and Christine O'Connor. This book is dedicated to all the candidates seeking CCSP certification; I hope it helps.

About the Author

Ben Malisow, CISSP, CISM, CCSP, SSCP, and Security+, is an instructor for (ISC)², teaching prep classes for the CISSP, CCSP, and SSCP certifications. He has been in the information technology and information security field for almost 25 years. He wrote the internal IT security policy for DARPA, served as the information system security manager for the FBI's most-classified counterterror intelligence-sharing network, and helped develop the IT security architecture for the Department of Homeland Security's Transportation Security Administration. Ben has taught courses at many schools and universities, including Carnegie Mellon's CERT/SEI, UTSA, the College of Southern Nevada, and grades 6–12 in the public school system in Las Vegas. He is widely published in the field, having written for SecurityFocus.com, *ComputerWorld*, and various other publications as well as several books. You can find his blog at Securityzed.com.

About the Technical Editor

Aaron Kraus began his career as a security auditor for US federal government clients. From there he moved into security risk management for healthcare and financial services, which offered more opportunities to travel, explore, and eat amazing food around the world. He currently works for a cyber risk insurance startup in San Francisco and spends his free time dabbling in cooking, cocktail mixology, and photography.

Contents at a Glance

<i>Introduction</i>	<i>xxi</i>
<i>Assessment Test</i>	<i>xxviii</i>
Chapter 1	Architectural Concepts 1
Chapter 2	Design Requirements 25
Chapter 3	Data Classification 43
Chapter 4	Cloud Data Security 71
Chapter 5	Security in the Cloud 93
Chapter 6	Responsibilities in the Cloud 123
Chapter 7	Cloud Application Security 149
Chapter 8	Operations Elements 181
Chapter 9	Operations Management 209
Chapter 10	Legal and Compliance Part 1 237
Chapter 11	Legal and Compliance Part 2 269
Appendix A	Answers to Written Labs 295
Appendix B	Answers to Review Questions 303
<i>Index</i>	<i>321</i>

Contents

Introduction

xxi

Assessment Test

xxviii

Chapter 1	Architectural Concepts	1
	Cloud Characteristics	2
	Business Requirements	4
	Existing State	5
	Quantifying Benefits and Opportunity Cost	6
	Intended Impact	8
	Cloud Evolution, Vernacular, and Models	9
	New Technology, New Options	9
	Cloud Computing Service Models	10
	Cloud Deployment Models	12
	Cloud Computing Roles and Responsibilities	13
	Cloud Computing Definitions	14
	Foundational Concepts of Cloud Computing	16
	Sensitive Data	16
	Virtualization	16
	Encryption	16
	Auditing and Compliance	17
	Cloud Service Provider Contracts	17
	Related and Emerging Technologies	18
	Summary	19
	Exam Essentials	19
	Written Labs	20
	Review Questions	21
Chapter 2	Design Requirements	25
	Business Requirements Analysis	26
	Inventory of Assets	26
	Valuation of Assets	27
	Determination of Criticality	27
	Risk Appetite	29
	Security Considerations for Different Cloud Categories	31
	IaaS Considerations	32
	PaaS Considerations	32
	SaaS Considerations	32
	General Considerations	33

	Design Principles for Protecting Sensitive Data	33
	Hardening Devices	33
	Encryption	35
	Layered Defenses	35
	Summary	36
	Exam Essentials	37
	Written Labs	37
	Review Questions	38
Chapter 3	Data Classification	43
	Data Inventory and Discovery	45
	Data Ownership	45
	The Data Lifecycle	46
	Data Discovery Methods	50
	Jurisdictional Requirements	51
	Information Rights Management (IRM)	53
	Intellectual Property Protections	53
	IRM Tool Traits	57
	Data Control	59
	Data Retention	60
	Data Audit	61
	Data Destruction/Disposal	63
	Summary	65
	Exam Essentials	65
	Written Labs	66
	Review Questions	67
Chapter 4	Cloud Data Security	71
	Cloud Data Lifecycle	73
	Create	74
	Store	75
	Use	75
	Share	75
	Archive	76
	Destroy	77
	Cloud Storage Architectures	78
	Volume Storage: File-Based Storage and Block Storage	78
	Object-Based Storage	78
	Databases	79
	Content Delivery Network (CDN)	79
	Cloud Data Security Foundational Strategies	79
	Encryption	79
	Masking, Obfuscation, Anonymization, and Tokenization	81
	Security Information and Event Management	84
	Egress Monitoring (DLP)	85

	Summary	86
	Exam Essentials	86
	Written Labs	87
	Review Questions	88
Chapter 5	Security in the Cloud	93
	Shared Cloud Platform Risks and Responsibilities	95
	Cloud Computing Risks by Deployment Model	97
	Private Cloud	98
	Community Cloud	98
	Public Cloud	100
	Hybrid Cloud	104
	Cloud Computing Risks by Service Model	104
	Infrastructure as a Service (IaaS)	104
	Platform as a Service (PaaS)	105
	Software as a Service (SaaS)	106
	Virtualization	106
	Threats	107
	Countermeasure Methodology	109
	Disaster Recovery (DR) and Business Continuity (BC)	112
	Cloud-Specific BIA Concerns	112
	Customer/Provider Shared BC/DR Responsibilities	113
	Summary	116
	Exam Essentials	116
	Written Labs	117
	Review Questions	118
Chapter 6	Responsibilities in the Cloud	123
	Foundations of Managed Services	126
	Business Requirements	127
	Business Requirements: The Cloud Provider Perspective	127
	Shared Responsibilities by Service Type	133
	IaaS	133
	PaaS	133
	SaaS	133
	Shared Administration of OS, Middleware, or Applications	134
	Operating System Baseline Configuration and Management	134
	Shared Responsibilities: Data Access	136
	Customer Directly Administers Access	137
	Provider Administers Access on Behalf of the Customer	137
	Third-Party (CASB) Administers Access on Behalf of the Customer	137

	Lack of Physical Access	137
	Audits	138
	Shared Policy	142
	Shared Monitoring and Testing	142
	Summary	143
	Exam Essentials	143
	Written Labs	144
	Review Questions	145
Chapter 7	Cloud Application Security	149
	Training and Awareness	151
	Common Cloud Application Deployment Pitfalls	154
	Cloud-Secure Software Development Lifecycle (SDLC)	156
	Configuration Management for the SDLC	157
	ISO/IEC 27034-1 Standards for Secure Application Development	158
	Identity and Access Management (IAM)	159
	Identity Repositories and Directory Services	160
	Single Sign-On (SSO)	161
	Federated Identity Management	161
	Federation Standards	162
	Multifactor Authentication	162
	Supplemental Security Components	163
	Cloud Application Architecture	164
	Application Programming Interfaces	164
	Tenancy Separation	165
	Cryptography	165
	Sandboxing	166
	Application Virtualization	167
	Cloud Application Assurance and Validation	167
	Threat Modeling	167
	Quality of Service	169
	Software Security Testing	170
	Approved APIs	172
	Software Supply Chain (API) Management	172
	Securing Open-Source Software	172
	Application Orchestration	173
	The Secure Network Environment	174
	Summary	175
	Exam Essentials	175
	Written Labs	176
	Review Questions	177

Chapter 8	Operations Elements	181
	Physical/Logical Operations	183
	Facilities and Redundancy	184
	Virtualization Operations	194
	Storage Operations	196
	Physical and Logical Isolation	199
	Application Testing Methods	200
	Security Operations Center	201
	Continuous Monitoring	201
	Incident Management	202
	Summary	203
	Exam Essentials	204
	Written Labs	204
	Review Questions	205
Chapter 9	Operations Management	209
	Monitoring, Capacity, and Maintenance	211
	Monitoring	211
	Maintenance	213
	Change and Configuration Management (CM)	217
	Baselines	218
	Deviations and Exceptions	218
	Roles and Process	219
	Release Management	221
	IT Service Management and Continual Service Improvement	222
	Business Continuity and Disaster Recovery (BC/DR)	223
	Primary Focus	224
	Continuity of Operations	225
	The BC/DR Plan	225
	The BC/DR Kit	227
	Relocation	228
	Power	229
	Testing	230
	Summary	231
	Exam Essentials	231
	Written Labs	232
	Review Questions	233
Chapter 10	Legal and Compliance Part 1	237
	Legal Requirements and Unique Risks in the Cloud	
	Environment	239
	Legal Concepts	239
	US Laws	242

International Laws	246
Laws, Frameworks, and Standards Around the World	246
Information Security Management Systems (ISMSs)	252
The Difference between Laws, Regulations, and Standards	254
Potential Personal and Data Privacy Issues in the Cloud Environment	254
eDiscovery	255
Forensic Requirements	256
Conflicting International Legislation	256
Cloud Forensic Challenges	257
Direct and Indirect Identifiers	258
Forensic Data Collection Methodologies	258
Audit Processes, Methodologies, and Cloud Adaptations	259
Virtualization	259
Scope	259
Gap Analysis	260
Restrictions of Audit Scope Statements	260
Policies	261
Different Types of Audit Reports	261
Auditor Independence	262
AICPA Reports and Standards	262
Summary	263
Exam Essentials	264
Written Labs	264
Review Questions	265
Chapter 11 Legal and Compliance Part 2	269
The Impact of Diverse Geographical Locations and Legal Jurisdictions	271
Policies	272
Implications of the Cloud for Enterprise Risk Management	276
Choices Involved in Managing Risk	276
Risk Management Frameworks	279
Risk Management Metrics	281
Contracts and Service-Level Agreements (SLAs)	281
Business Requirements	284
Cloud Contract Design and Management for Outsourcing	284
Identifying Appropriate Supply Chain and Vendor Management Processes	285
Common Criteria Assurance Framework (ISO/IEC 15408-1:2009)	285

	CSA Security, Trust, and Assurance Registry (STAR)	286
	Supply Chain Risk	287
	Manage Communication with Relevant Parties	288
	Summary	289
	Exam Essentials	289
	Written Labs	289
	Review Questions	290
Appendix A	Answers to Written Labs	295
	Chapter 1: Architectural Concepts	296
	Chapter 2: Design Requirements	296
	Chapter 3: Data Classification	297
	Chapter 4: Cloud Data Security	298
	Chapter 5: Security in the Cloud	299
	Chapter 6: Responsibilities in the Cloud	299
	Chapter 7: Cloud Application Security	300
	Chapter 8: Operations Elements	300
	Chapter 9: Operations Management	301
	Chapter 10: Legal and Compliance Part 1	302
	Chapter 11: Legal and Compliance Part 2	302
Appendix B	Answers to Review Questions	303
	Chapter 1: Architectural Concepts	304
	Chapter 2: Design Requirements	305
	Chapter 3: Data Classification	307
	Chapter 4: Cloud Data Security	308
	Chapter 5: Security in the Cloud	310
	Chapter 6: Responsibilities in the Cloud	311
	Chapter 7: Cloud Application Security	313
	Chapter 8: Operations Elements	314
	Chapter 9: Operations Management	316
	Chapter 10: Legal and Compliance Part 1	317
	Chapter 11: Legal and Compliance Part 2	319
	<i>Index</i>	321

Introduction

The Certified Cloud Security Professional (CCSP) certification satisfies the growing demand for trained and qualified cloud security professionals. It is not easy to earn this credential; the exam is extremely difficult, and the endorsement process is lengthy and detailed.

The *CCSP (ISC)² Official Study Guide* offers the cloud professional a solid foundation for taking and passing the Certified Cloud Security Professional (CCSP) exam. However, if you plan on taking the exam to earn the certification, this cannot be stressed enough: **you cannot expect to pass the exam using this book as your sole source.** Please refer to the list of additional recommended reading at the end of this introduction.

(ISC)²

The CCSP exam is governed by (ISC)². (ISC)² is a global not-for-profit organization with four primary mission goals:

- Maintain the Common Body of Knowledge (CBK) for the field of information systems security.
- Provide certification for information systems security professionals and practitioners.
- Conduct certification training and administer the certification exams.
- Oversee the ongoing accreditation of qualified certification candidates through continued education.

A board of directors elected from the ranks of its certified practitioners operates the (ISC)².

(ISC)² supports and provides a wide variety of certifications, including the CISSP, SSCP, CAP, CSSLP, HCISPP, and CCSP. These certifications are designed to verify the knowledge and skills of IT security professionals across all industries. You can obtain more information about the organization and its other certifications by visiting www.isc2.org.

Topical Domains

The CCSP certification covers material from the six topical domains. They are as follows:

- Domain 1: Cloud Concepts, Architecture, and Design
- Domain 2: Cloud Data Security
- Domain 3: Cloud Platform and Infrastructure Security
- Domain 4: Cloud Application Security
- Domain 5: Cloud Security Operations
- Domain 6: Legal, Risk, and Compliance

These domains cover all of the pertinent areas of security related to the cloud. All the material in the certification are vendor- and product-agnostic. Each domain also contains a list of topics and subtopics the CCSP-certified professional is expected to know.

The detailed list of domains/topics of knowledge, experience requirements, exam procedures, and exam domain weights can be found in the CCSP Certification Exam Outline: <https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CCSP-Exam-Outline.ashx>.

Prequalifications

(ISC)² has defined the qualifications and requirements you must meet to become a CCSP:

- A minimum of five years of cumulative, paid, full-time information technology experience of which three years must be in information security and one year in one of the six domains of the CCSP examination
- Earning the Cloud Security Alliance's CCSK certificate may be substituted for one year of experience in one of the six domains of the CCSP examination.
- Earning the CISSP credential may be substituted for the entire CCSP experience requirement.

Candidates who do not meet these requirements may still sit for the exam and become an Associate of (ISC)². Associates have six years (from passing the exam) to fulfill any remaining experience requirements.

Certified members of (ISC)² must also adhere to the (ISC)² formal code of ethics, which can be found on the (ISC)² website at www.isc2.org/ethics.

Overview of the CCSP Exam

The CCSP exam typically consists of 125 multiple-choice questions covering the six domains of the CCSP CBK, and you must achieve a score of 70 percent or better to pass.

You will have three hours to complete the exam. Twenty-five of the questions will be unscored questions used solely for research purposes. Be sure to answer every question as best you can because you will not know which questions are scored and which are not and you will receive 0 points for unanswered questions. Points are not subtracted for incorrect answers; never leave any question unanswered, even if your answer is a guess.

CCSP Exam Question Types

Most of the questions on the CCSP exam are in the multiple-choice format, with four options and a single correct answer. Some are straightforward, such as asking you to

identify a definition. Other questions will ask you to identify an appropriate concept or best practice. Here is one example:

1. Putting sensitive operational information in a database away from the production environment in order to provide higher protection and isolation is called _____.
- A. Randomization
 - B. Elasticity
 - C. Obfuscation
 - D. Tokenization

You must select the one correct or best answer. Sometimes the answer will seem obvious to you, and other times it will be harder to discriminate between two good answers and pick the best. Watch out for general, specific, universal, superset, and subset answer selections. In other cases, none of the answers will seem correct. In these instances, you will want to select the least incorrect answer. There are also questions that are based on theoretical scenarios, where you must answer several questions given a specific situation.



The correct answer to the question above is option D, tokenization. In a tokenized arrangement, sensitive information is placed in a database away from the production environment, and tokens (representing the stored sensitive information) are stored in a database within the production environment. In order to select the correct answer, the reader has to understand how tokenization works and how that method can be used to isolate sensitive data from the production environment; the question does not mention tokens or tokenization, so it requires complex thought. An easier answer would be “data segregation,” but that’s not an option. This is not an easy question.

In addition to the standard multiple-choice question format, (ISC)² has added a new question format that uses a drag-and-drop approach. For instance, you may see a list of items on one side of the screen that you need to drag and drop onto their appropriate counterparts on the other side of the screen. Other interactive questions may include matching terms with definitions and clicking on specific areas of a chart or graphic. These interactive questions are weighted with a higher point value than the multiple-choice type, so you should pay extra attention when answering them.

Study and Exam Preparation Tips

I recommend planning for at least 30 days of intensive studying for the CCSP exam. I have compiled a list of tips that should help:

- Take one or two evenings to read each chapter thoroughly and work through the review material at the end.

- Think about joining a study group, to share insight and perspective with other candidates.
- Answer all the review questions and take the practice exams on the Sybex website associated with this book (see details on the back cover).
- Complete the written labs from each chapter.
- Before you move on to the next section of work, be sure to review the previous day's study to be sure you are retaining the information.
- Take study breaks but stay on track.
- Put together a study plan.
- Review the (ISC)² Exam Outline.

Advice on Taking the Exam

Here are some test-taking tips and general guidelines:

- Answer easy questions first. You can mark all of the questions you are unsure of and go back over them after you have completed the exam.
- Eliminate incorrect answers first.
- Be careful of double negatives in the language of the question.
- Read the questions carefully to ensure you fully understand them.
- *Take your time.* Do not hurry. Rushing leads to test anxiety and loss of focus.
- Take a bathroom break and a breather if you need to, but keep it short. You want to maintain your focus.
- Observe all exam center procedures. Even if you've previously taken an exam at a Pearson Vue center, some have slightly different requirements.

Manage your time. You have three hours to answer 125 questions. That equates to just a bit less than two minutes per question, which in most cases is more than enough time.

Make sure you get plenty of sleep the night before. Be sure to bring any food or drink you think you might need, although they will be stored while you are taking the exam. Also, remember to bring any medications you need to take and alert the staff of any condition that might interfere with your test taking, such as diabetes or heart disease. No test or certification is worth your health.

You may not wear a watch into the test lab. There are timers on the computers and in the testing labs. You must also empty your pockets, with the exception of your locker key and ID.

You must bring at least one picture ID with a signature, such as a driver's license, with you to the testing center, and you should have at least one more form of ID with a signature. Arrive at least 30 minutes early to the testing site to make sure you have everything you need. Bring the registration form that you received from the testing center along with your IDs.

Completing the Certification Process

Once you have successfully completed the CCSP exam, there are a few more things to do before you have earned your new credential. First, transmission of your (ISC)² score happens automatically. You will receive instructions on the printed results from your test as you leave the testing center. They will include instructions on how to download your certification form, which will ask you for things such as whether you already have another (ISC)² credential (such as the CISSP) and similar questions. Once completed, you will need to sign and submit the form to (ISC)² for approval. Usually, you will receive notice of your official certification within three months. Once you are fully certified, you can use the CCSP designation in your signatures and other places of importance, per (ISC)² usage guidelines.

Notes on This Book's Organization

This book covers all of the six CCSP Common Body of Knowledge (CBK) domains in sufficient depth to provide you with a basic understanding of the necessary material. The main body of the book is composed of 11 chapters that are arranged as follows:

Chapter 1: Architectural Concepts

Chapter 2: Design Requirements

Chapter 3: Data Classification

Chapter 4: Cloud Data Security

Chapter 5: Security in the Cloud

Chapter 6: Responsibilities in the Cloud

Chapter 7: Cloud Application Security

Chapter 8: Operations Elements

Chapter 9: Operations Management

Chapter 10: Legal and Compliance Part 1

Chapter 11: Legal and Compliance Part 2

Obviously, the book does not follow the order of the domains or the official exam outline. Instead, the chapters of the book are arranged in a way to explain the material in a narrative format that conveys the concepts in a linear manner.

Each chapter includes elements designed to assist you in your studies and to test your knowledge of the material presented in the chapter. It is recommended that you read Chapter 1 first to best orient yourself in the subject matter before moving on to the other chapters.



Please see the table of contents and chapter introductions for more detailed domain topics covered in each chapter.

Elements of This Study Guide

This study guide contains several core elements that will help you prepare for the CCSP exam and the real world beyond it:

Real World Scenarios: The book has several real-world scenarios laid out to help you further assimilate the information by seeing where and under what circumstances certain solutions have worked (or not) in the real world and why.

Summaries: The summary is a quick overview of important points made in the chapter.

Exam Essentials: Exam Essentials highlight topics that could appear on the exam in some form. While the author does not know exactly what will be included on a particular exam, this section reinforces significant concepts that are crucial to understanding the CBK and the test specifications for the CCSP exam.

Written Labs: Each chapter includes written labs that bring together various topics and concepts brought up in the chapter. While this content is designed for classroom use in a college/university, it may aid in your understanding and clarification of the material beyond classroom use as well.

Answers to the Written Labs are in Appendix A.

Chapter Review Questions: Each chapter includes practice questions designed to measure your knowledge of fundamental ideas discussed in the chapter. After you finish each chapter, answer the questions; if some of your answers are incorrect, it is an indication that you need to spend more time studying the corresponding topics. The answers to the practice questions are in Appendix B.

What Is Included with the Additional Study Tools

Beyond all of the information provided in the text, this book comes with a helpful array of additional online study tools. All of the online study tools are available by registering your book at www.wiley.com/go/sybextestprep. You'll need to choose this book from the list of books there, complete the required registration information, including answering the security verification to prove book ownership. After that you will be emailed a pin code. Once you get the code, follow the directions in the email or return to www.wiley.com/go/sybextestprep to set up your account using the code and get access.

The Sybex Test Preparation Software

The test preparation software, made by the experts at Sybex, can help prepare you for the CCSP exam. In this test engine, you will find all the review and assessment questions from the book and additional bonus practice exam questions that are included with the study

tools. You can take the assessment test, test yourself by chapter, take the practice exam, or take a randomly generated exam consisting of all the questions.

Glossary of Terms in PDF

Sybex offers a robust glossary of terms in PDF format. This comprehensive glossary includes essential terms you should understand for the CCSP certification exam, in a searchable format.

Bonus Practice Exams

Sybex includes two practice exams; these contain questions meant to survey your understanding of the essential elements of the CCSP CBK. Both tests are 125 questions long, the length of the actual certification exam. The exams are available online at www.wiley.com/go/sybextestprep.

Assessment Test

1. What type of solutions enable enterprises or individuals to store data and computer files on the Internet using a storage service provider rather than keeping the data locally on a physical disk such as a hard drive or tape backup?
 - A. Online backups
 - B. Cloud backup solutions
 - C. Removable hard drives
 - D. Masking
2. When using an infrastructure as a service (IaaS) solution, which of the following is not an essential benefit for the customer?
 - A. Removing the need to maintain a license library
 - B. Metered service
 - C. Energy and cooling efficiencies
 - D. Transfer of ownership cost
3. _____ focuses on security and encryption to prevent unauthorized copying and limitations on distribution to only those who pay.
 - A. Information rights management (IRM)
 - B. Masking
 - C. Bit splitting
 - D. Degaussing
4. Which of the following represents the correct set of four cloud deployment models?
 - A. Public, private, joint, and community
 - B. Public, private, hybrid, and community
 - C. Public, Internet, hybrid, and community
 - D. External, private, hybrid, and community
5. What is a special mathematical code that allows encryption hardware/software to encrypt and then decipher a message?
 - A. PKI
 - B. Key
 - C. Public-private
 - D. Masking