IN THIS CHAPTER

- Learning about the (ISC)² and the CCSP certification
- Understanding the benefits of getting certified
- Exploring the CCSP certification domains
- Creating a study plan
- Registering for the CCSP exam
- Taking the CCSP exam

Chapter 1

Familiarizing Yourself with (ISC)² and the CCSP Certification

In this chapter, you develop an understanding of the (ISC)² organization and CCSP certification, including what you need to know before the exam, what to expect during the exam, and what to do after you pass the exam!

Appreciating (ISC)² and the CCSP Certification

The *International Information System Security Certification Consortium* — more easily referred to as (ISC)² — is a nonprofit organization that has been training and certifying cybersecurity professionals since 1989. With more than 190,000

certified members and associates worldwide, (ISC)² is widely regarded as the world's leading cybersecurity professional organization. Its flagship certification, launched in 1994, is the Certified Information System Security Professional (CISSP). Since then, the organization has launched other certifications, including three CISSP concentrations. As of today, (ISC)² offers the following ten professional certifications and concentrations:

- Certified in Cybersecurity (CC)
- Certified Information Systems Security Professional (CISSP)
  - Information Systems Security Architecture Professional (CISSP-ISSAP)
  - Information Systems Security Engineering Professional (CISSP-ISSEP)
  - Information Systems Security Management Professional (CISSP-ISSMP)
- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- HealthCare Information Security and Privacy Practitioner (HCISSP)

In addition to managing a broad assortment of cybersecurity certifications, (ISC)² also organizes the annual (ISC)² Security Congress conference, which provides continuing education, networking, and career advancement opportunities for thousands of security professionals every year.

In 2015, (ISC)² and the Cloud Security Alliance (CSA) introduced the Certified Cloud Security Professional (CCSP) certification to the world. The CCSP is a standalone credential, but builds on certifications like the CISSP and CSA's Certificate of Cloud Security Knowledge (CCSK). The main objective of the CCSP is to certify that the credential holder has the knowledge, skills, and experience required to design, manage, and secure data in cloud-based applications and infrastructures.

Knowing Why You Need to Get Certified

According to (ISC)², a CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. In preparing for the CCSP exam, you expand your knowledge of information security and cloud computing concepts,

making you a more well-rounded professional, while also improving your job security. Achieving the CCSP credential is a great way to strut your stuff in front of employers who seek verified cloud security expertise — say hello to increased visibility and new career opportunities!

REMEMBER

While the CCSP isn't generally a strict requirement for most cloud security positions, it does differentiate you to potential employers. It shows that you have the technical skills and experience they need as they seek to securely build and manage their cloud environments. The CCSP is a vendor-neutral certification, meaning the knowledge and skills it certifies can be applied to various technologies and methodologies. By not being limited to a single vendor, the CCSP designation is as versatile as it is valuable and can help you start or build a long-lasting career in cloud security.

Studying the Prerequisites for the CCSP

Along with passing the CCSP exam, you must satisfy a few other requirements to achieve the CCSP designation. As a CCSP candidate, you must have at least five years of paid work experience in Information Technology, and at least three of those years must include Information Security experience. Further, you must have at least one year of experience working in one or more of the six domains of the CCSP Common Body of Knowledge (CBK).

(ISC)² emphasizes practical, real-world experience to fulfill the work experience requirements. In other words, it's not enough to have IT or Information Security listed as a line-item on your resume — you must have regularly applied relevant knowledge and skills to perform your job duties. Some examples of full-time jobs that may satisfy these requirements include, but aren't limited to

- Cloud architect
- Enterprise architect
- Information systems security officer
- Security administrator
- Security analyst
- Security engineer
- Systems architect
- Systems engineer

If you don't have acceptable full-time work experience, (ISC)² also accepts part-time work and internships under the following guidelines:

- **Part-time:** 2,080 hours of part-time work equals one year of full-time experience.
- **Internships:** For paid or unpaid internships, you must provide documentation on company letterhead that confirms your experience.


TIP

If you already hold CSA's CCSK certificate, (ISC)² waives the requirement for one year of experience in one or more of the six CCSP domains. Even better, if you hold the CISSP credential, then you're all set for 100 percent of the CCSP experience requirements!


TIP

If you don't already have the required work experience, you can still take the CCSP exam. When you pass, you'll earn the Associate of (ISC)² designation and be given six years to earn the required experience and become a fully certified member. You can learn more about CCSP experience requirements at `www.isc2.org/Certifications/CCSP/experience-requirements`.

Understanding the CCSP Domains

Six security domains are within the CCSP Common Body of Knowledge (CBK), and I cover them fully in Chapters 3 through 14. Think of these domains as the six subject areas that you must master in order to pass the exam. The CCSP domains (and their respective weightings on the exam) are

- **Domain 1:** Cloud Concepts, Architecture, and Design (17 percent)
- **Domain 2:** Cloud Data Security (20 percent)
- **Domain 3:** Cloud Platform and Infrastructure Security (17 percent)
- **Domain 4:** Cloud Application Security (17 percent)
- **Domain 5:** Cloud Security Operations (16 percent)
- **Domain 6:** Legal, Risk and Compliance (13 percent)

Domain 1: Cloud Concepts, Architecture, and Design

Domain 1: Cloud Concepts, Architecture, and Design counts for 17 percent of the CCSP exam and is the foundational domain that lays the groundwork for your

understanding of cloud computing. You should think of this domain as your gateway to cloud mastery — everything else simply builds on the elements and concepts outlined here.

In this domain, you learn how to identify and define everyone's role in a cloud implementation, including both the cloud provider and cloud customer. Domain 1 gives you an understanding of the key technical characteristics of cloud computing and also introduces you to the various capabilities, categories, and deployment models of cloud architectures.

You must consider specific design requirements in order to develop a functional and secure cloud environment. Some of these requirements coincide with your traditional data center, so you should see some familiar content. However, certain features of cloud computing require additional consideration and new approaches. Domain 1 introduces the cloud security data lifecycle and discusses how things like cryptography, network security, and access control should be used to protect against the many unique threats that cloud environments and cloud data face.

Domain 1 also introduces various methods for cloud customers to evaluate and verify cloud providers against established security standards and certifications. Cloud customers cannot manage and control cloud environments the way they control their data centers, so there needs to be a way for them to validate the security and operations of the cloud services they use. Cloud providers can earn certifications across their entire environments and applications, or they can opt for various certifications aimed at specific components and products, such as FIPS 140-3 certification. You learn about all of these topics in Domain 1.

Domain 2: Cloud Data Security

Domain 2: Cloud Data Security is the most heavily weighted domain on the CCSP exam, at 20 percent, and covers identifying, classifying, and securing cloud data. The domain begins with coverage of the cloud data lifecycle and identifies the most important security considerations, from data creation through data destruction.

Each of the cloud service categories (IaaS, PaaS, and SaaS) leverages its own data storage types. Domain 2 defines these types, identifies the threats they face, and explores various unique considerations around securing each of them. While many of the data security technologies used in the cloud are similar to those used in traditional data centers, how they are used varies based on the specific cloud architecture and any regulatory or contractual obligations the cloud provider may have. This domain covers designing and implementing a data security strategy that fits your particular cloud architecture.

The topics of data discovery and data classification are core to any data security strategy. Domain 2 explores these concepts as they pertain to cloud computing and focuses on the cloud-specific challenges associated with each. Here, you learn how multitenancy and the large geographic footprint of most cloud providers make discovering and classifying sensitive data a big challenge and what to do about that. Among the many solutions, this domain covers Information Rights Management (IRM) technologies and how they can be used to enforce specific security and privacy requirements for data in (or outside of) the cloud. In addition to protecting data, this domain covers the concepts of data retention, deletion, and archiving.

Ensuring effective data security also requires that you ensure the auditability, traceability, and accountability of data events. Domain 2 covers the identification of data sources by cloud service category, and the logging, storing, and analyzing of relevant data events. Among the many requirements you explore, this domain emphasizes ensuring chain of custody and nonrepudiation for data events. Don't worry, Chapters 5 and 6 cover all this jargon, and more!

Domain 3: Cloud Platform and Infrastructure Security

Cloud Platform and Infrastructure Security (Domain 3) counts for 17 percent of the CCSP exam and focuses on the practical matters of securing a cloud platform and its infrastructure. You explore what makes up a cloud's virtualized (logical) environment and how that relates to the physical environment underneath it — you also dive into what it takes to secure both the logical and physical components of a cloud environment.

In Domain 1, you focus a lot of your attention on the architecture of cloud environments. It's there that you learn about the virtual infrastructure that enables the power of cloud computing, and appreciate how the underlying physical infrastructure supports all that cloudy goodness. In Domain 3, you explore the unique security concerns and requirements associated with a cloud's logical and physical environment. Mastery of these concepts requires that you understand a host of cloud-specific risks, including virtualization risks, and learn what security controls and strategies to implement as a result. In Domain 3, you learn all about what it takes to design a secure data center at the logical and physical layers.

A major component of any secure system is ensuring appropriate identity and access management. This domain hits on identification, authentication, and authorization for cloud infrastructures and covers how these topics should be managed by cloud customers who rely on a shared, third-party resources, like the cloud.

Last, but not least, Domain 3 covers the essential topics of business continuity and disaster recovery (BCDR). These concepts are hugely important for any company on any kind of architecture — cloud or legacy. While cloud environments inherently provide a great deal of redundancy over traditional data centers, organizations must understand how cloud usage fits into their overall BCDR strategy. This domain dives into what it takes to develop a comprehensive strategy, including defining your scope, generating your requirements, and appropriately assessing BCDR risks to your organization. While an effective strategy requires lots of planning, it's also important that your plan is regularly tested to ensure its feasibility and effectiveness.

Domain 4: Cloud Application Security

Domain 4: Cloud Application Security is weighted at 17 percent of the CCSP exam and covers the most critical application security concerns that are relevant to cloud environments. This domain starts with coverage of common cloud-related application security pitfalls and then introduces some of the most significant categories of cloud application vulnerabilities.

One of the primary focal points of Domain 4 is the secure software development lifecycle (SDLC) process. In this domain, you learn all about the phases of that process and how to apply it to secure application development in cloud environments. You not only explore the most common SDLC methodologies (waterfall and agile), but you also take a look at threat modeling and explore how it pertains to secure cloud development and configuration management.

A major part of software development, whether in cloud environments or not, is application testing. In Domain 4, you learn about static and dynamic application security testing (SAST and DAST) — you gain an understanding of the pros and cons of each and how they can be used together to form a comprehensive cloud application testing strategy. You learn about the differences of black box and white box testing and identify when to use each method. To wrap up your study of security testing methodologies, Domain 4 introduces the practices of vulnerability scanning and penetration testing. You learn that these are not the same things and gain an appreciation for how they complement each other as part of your comprehensive application testing strategy.

Between Domain 1 and Domain 4, you learn that cloud environments and applications can be made up of multiple components, services, and integrations from various sources. In this domain, you explore the importance of using verified secure software components. You dive into topics like supply-chain management and third-party software management and gain an understanding of using secure and approved Application Programming Interfaces (APIs) and Open Source Software (OSS). After laying this groundwork, Domain 4 covers the architecture of

cloud applications and highlights specific security components that you should understand. In this domain, you revisit topics like cryptography and Identity and Access Management (IAM) and learn how they apply specifically to cloud-based application development.

Domain 5: Cloud Security Operations

Domain 5 covers the broad topic of security operations in the cloud, which includes everything from managing your data center's security to collecting and preserving digital evidence using cloud forensics techniques. This domain is worth 16 percent of the total CCSP exam.

Domain 5 begins with coverage of topics related to implementing and building a cloud infrastructure, both at the physical and logical layers. You learn about secure hardware configuration requirements (such as BIOS security) and also explore how to securely install and configure virtualization management tools. Next, the domain takes you from building your cloud infrastructure to securely operating it. This domain covers the nitty-gritty details associated with access controls for local and remote access, securing your network configurations, and using baselines as a guide, to harden the operating systems throughout your cloud environment. You learn how to securely manage stand-alone hosts, clustered hosts, as well as guest operating systems on the virtualized infrastructure.

Aside from building and operating a secure cloud infrastructure, Domain 5 has a strong focus on securely managing your physical and logical cloud infrastructure, which includes all of the technical, management, and operational activities and controls necessary to keep your cloud environment securely running. This domain covers things like patch management, performance and capacity monitoring, hardware monitoring, and backup and restore functions. You spend some time learning about additional network security controls, like honeypots and network security groups, and also learn about securing and securely using the management plane. Much of this information feeds into the domain's coverage of the Security Operations Center (SOC) and how a SOC can be used to monitor security controls across a cloud's physical and logical environment.

One of the most important aspects of Domain 5 involves coverage of operational controls and standards, like ITIL, and how to apply and implement those standards in your cloud environment. You explore common IT topics like change management, incident management, and configuration management, as they specifically pertain to cloud computing. Domain 5 wraps up with an important discussion about managing communication with customers, vendors, and other relevant parties.

Domain 6: Legal, Risk, and Compliance

Domain 6 counts for roughly 13 percent of the CCSP exam and focuses on the many legal and regulatory requirements that pertain to cloud environments. Cloud computing environments often extend across national borders and are subject to multiple different jurisdictions and regulations. You can picture one big cloud that's hovering over three different countries. Each country has its own regulations and policies, and within that country are several different states or jurisdictions that have their own laws. If that's not enough, there are also regulations specific to banking, healthcare, education, and the list goes on — but there's just that one large cloud hovering above, trying to cover everyone down below. Yikes! Maintaining compliance in each territory and industry can be overwhelming. This domain focuses on how cloud providers and customers can handle all their legal, risk, and compliance obligations.

In Domain 6, you learn that a pretty common legal challenge in cloud computing comes in the form of an e-Discovery order to produce data for a court or other government entity. In this domain, you examine the notion of e-Discovery and digital forensics in the cloud, as well as the challenges that come with it.

It's not good enough for cloud providers to do a bunch of security things and tell their customers trust them — auditing is a huge part of maintaining and demonstrating compliance to regulators and customers. This domain explores the different types of audits and how they impact cloud environments and their design. You explore the auditing process, standards that govern the process, reporting, and the stakeholders involved.

In addition to legal and regulatory requirements, Domain 6 covers the subject of risk management as it pertains to cloud computing. Cloud computing creates a paradigm shift from owning and controlling everything to the Shared Responsibility Model (don't worry, I discuss this in Chapter 3). With this change, customers need to think about how they assess, manage, and monitor risk different than they ever have. Domain 6 includes various risk frameworks and focuses on applying them in the cloud.

Preparing for the Exam

You can prepare for the CCSP exam in many ways. Self-study (like reading this book) is a very popular way to prepare, but you can include lots of other components in your study plan. Whether it's practical hands-on experience at work (which is not only helpful, but a requirement for certification) or formal classroom training, you should put together a mix of study elements that works best for your personal learning style.

TIP

When preparing for the CCSP exam, I recommend that you establish and commit to a study plan. Your study plan should include a firm timeline, study materials of choice, studying methodology, and your selected method(s) of practicing. I recommend either a 90-day or 120-day timeline, depending on your level of experience. If you've already passed the CISSP or have many years of Information Security experience, then a 90-day plan should suffice. If you're starting from a more junior level, consider giving yourself a full four months. The key is to set an aggressive timeline that is realistic based on your current knowledge and time commitments. Make sure that you consider your planned work and family commitments. I will not be held accountable for angry husbands, wives, children, or pets!

TIP

To successfully prepare for the CCSP exam, you really have to know your learning style and cater to it. Personally, I learn best by locking myself in a room and reading books in silence. Other people prefer small study groups, and some opt for classroom learning. I present some options in the following sections, but it's up to you to find the ones that work best for you.

Studying on your own

Self-study is probably the most common way for people to prepare for the CCSP and other exams like it. Many self-study resources are available for you, including books, practice exams, and a host of Internet resources. (See Appendix B for some resources that complement this book.)

Your first step should be to download the official CCSP Certification Exam Outline (`www.isc2.org/CCSP-Exam-Outline`). I've aligned this book with the topics in that document, and it's a good idea to review it to get an idea of the subjects that you're about to learn.

Your next step is my personal favorite: Read this book. *CCSP For Dummies* is $(ISC)^2$-approved and covers of the content in the CCSP CBK. By starting with this book, you get a thorough review of all the topics that you can expect when you sit for the CCSP exam. It doesn't matter if you read *CCSP For Dummies* cover to cover or hop around the chapters out of order — the book is modular and meant to be read in any way you want, although upside-down might be a bit tough!

REMEMBER

The purchase of this book grants you access to online practice questions and flashcards (see the Introduction for more information). Use these resources to assess your learning after you complete the book.

After reading this book, you should then read any other study resources you can get your hands on to strengthen your understanding and retention of the exam topics. Additional resources can include other books (just make sure they're

(ISC)²-approved!), web resources (see Appendix B), or the wealth of resources that ISC2 recommends on its website (www.isc2.org/certifications/References).

WARNING

Don't rely on any single book (including this awesome one!) as your only resource to prepare for the CCSP. The exam covers a wide range of information, and you should get multiple views to ensure you fully understand each topic.

Another key to self-study is validating that you've learned and retained critical information. You should answer a whole lot of practice questions. In addition to the ones that come with this book, lots of resources are available for CCSP practice exams and questions. (Check out Appendix B to get you started.) You should know that no practice exams perfectly mirror the CCSP exam — some may be unbearably difficult, while others fail to cover half the exam topics. That's why I recommend answering as many practice questions from as many sources possible — just make sure that you get your practice questions and exams only from trusted sources.

Once you've read through all your study materials and you've tested your knowledge with practice questions, you should revisit this book one last time before taking the exam. Maybe you just focus on any notes you've taken in the margins or perhaps you do a quick reread of the entire book. Either way, I recommend revisiting this book closer to test day to remind yourself of any details you may have forgotten and clarify any topics that are still fuzzy.

Learning by doing

As Julius Caesar once said, "Experience is the best teacher." You could read all the cloud security books in the world, but nothing compares to practical hands-on learning.

You might work in a role in which you can use all of the things you learn in this book. If so, you're really lucky! Use every opportunity you get to apply the wealth of information from this book to what you do at work. If you don't have a related role, that's fine, too. Perhaps your company is migrating to the cloud? Or maybe your business already uses cloud services? Find teams and people involved in your organization's cloud endeavors and seek ways to get involved.

Getting official (ISC)² CCSP training

While many people are successful using self-study resources to prepare for the CCSP, some opt to attend a seminar or boot camp to brush up on the topics covered in the CCSP CBK. If you're in the latter group, (ISC)² offers multiple training

options to fit your learning style and schedule. For the most flexibility, you can choose (ISC)²'s self-paced training option. Self-paced training includes online access to recorded instruction and course content, chapter quizzes, learning activities, and more. The course costs $920 for 180 days of access. The course also qualifies you to receive 40 Continuing Professional Education (CPE) credits. This is a great access-anywhere option that puts you in complete control of your learning journey.

Some people learn best in a traditional classroom setting, and (ISC)² has an answer for that, too. You can sign up for classroom-based training led by (ISC)² or an official (ISC)² training provider. These are offered on-site — at an (ISC)² classroom or partner facility — as five- or six-day training seminars that cover the entire CCSP CBK in less than a week.

TIP

(ISC)² also offers private on-site training for groups of ten or more. This is ideal if your organization wants to train an entire team at once as(ISC)² sends an authorized instructor to the location of your choosing. If you're looking for the best of both worlds, (ISC)² offers an option that is led by an authorized instructor, but accessed from the comfort of your own home (or wherever you might be). You can choose a university-style course that meets online with a variety of scheduling options, including weekdays, weekends, and evenings.

You can find course schedules, costs, and additional information regarding official (ISC)² training at `www.isc2.org/training`.

Attending other training courses

While (ISC)² and their official partners provide excellent training courses, other legitimate organizations also offer quality training options. As any IT certification grows in popularity, so do the number of companies offering training services — it never fails.

REMEMBER

Make sure that you do your research before handing over your hard-earned money to one of these companies. Search online to learn more about the company and course instructor. Ask your friends and colleagues whether they've taken the course or had any experiences with the training organization. Get as much information as possible to make sure the company is reputable and the training is useful.

Practice, practice, practice

Practice questions are the best way to confirm that you understand the topics that you'll be tested on when you take the CCSP exam. You should definitely start with

the practice questions included with this book (see the Introduction for more information). After that, you can search for additional sample questions and practice exams — just make sure you're using reputable sources. When answering practice questions, make note of the types of questions you get wrong and revisit those topics in this book and your other study materials.

TIP

It's a good idea to time yourself when taking practice exams. You have four hours to answer 150 questions on the real exam, so make sure you're averaging under roughly 90 seconds per question.

Ensuring you're ready for the exam

Okay, so you read this book and answered the included practice questions. Then you read some more books and took additional practice exams. Maybe you found a CCSP study group or perhaps you decided to take a five-day bootcamp — when are you ready for the exam? You could easily study for months on end and spend lots of money on study material, but at some point, you just have to challenge the exam.

I recommend laying out a 90- or 120-day study plan and sticking to it. *CCSP For Dummies* has all the information you need to pass the CCSP exam. Read this book, take plenty of notes, and answer the practice questions until you grasp the content. Follow up by reading other books and study materials, and answering as many other practice questions as possible.

REMEMBER

The key to any effective plan is having a clear end-goal. Once you can consistently score 85 percent in each domain, I'd say you're ready for the exam!

Registering for the Exam

I recommend picking an exam date and registering for the exam at the beginning of your CCSP journey. The sooner you decide to register, the sooner you can have a firm goal to work toward!

TIP

Exam prices, taxes, and currency depend on your location. The current exam fee is $599 in the United States.

The CCSP exam is a computer-based test (CBT) and can be taken at a Pearson VUE testing center nearest you; Pearson VUE is the exclusive administrator for all (ISC)² exams around the world.

Registering for the exam is pretty easy if you follow these steps:

1. **Navigate to the Pearson VUE website by visiting `www.pearsonvue.com/isc2`.**
2. **Create an account for yourself with Pearson VUE.**
3. **Select the exam you're registering for.**

   Hopefully that's the CCSP, or else I'm writing the wrong book!
4. **Find the day, time, and Pearson VUE testing center that works best for you.**
5. **Pay your exam fee and register for the exam.**


TIP

(ISC)² offers reasonable and appropriate accommodations for test takers who have a legitimate need for special accommodations (such as a medical condition, for example). If you require special accommodations, contact (ISC)² before registering for your exam. Visit `www.isc2.org/Register-for-Exam` for more information.


WARNING

If you arrive at your test center more than 15 minutes after your scheduled exam time, you'll be considered late. If this happens, the testing center may choose to turn you away. If you're deemed late or if you miss the exam, you can kiss your exam fee goodbye!

You can reschedule or cancel your exam by contacting Pearson VUE, by phone, at least 24 hours before your scheduled exam. If you want to reschedule or cancel online, you have up to 48 hours before your scheduled exam to do so. Pearson VUE charges $50 to reschedule your exam, while it will run you $100 to cancel.

Taking the Exam

The CCSP is a computer-based testing (CBT) exam that consists of 150 multiple-choice questions. You have a maximum of four hours to complete the exam — that's about 96 seconds per question. (ISC)² uses a scaled scoring approach and requires you to achieve at least 700 out of a possible 1,000 points to pass the CCSP exam.


TECHNICAL STUFF

On every CCSP exam, 50 of the 150 questions are known as pre-test items that are included for research purposes only. Pre-test items do not count toward your score and are used by (ISC)² to try new questions. You won't know which questions are pre-test items, so it's important that you do your best to answer each of the 150 questions accurately.

TIP

If you've never taken a CBT exam, you can watch a demo and take a tutorial on the Pearson Vue website by visiting `www.pearsonvue.com/athena/athena.asp`.

When you get to the Pearson Vue testing center, you must check in before sitting for the exam. The standard check-in process involves the following steps:

- Present two forms of ID (refer to the (ISC)^2 website or your exam confirmation email for acceptable forms of ID.
- Have your photo taken.
- Provide your signature.
- Submit to a palm scan (unless it's prohibited by law).

Before your exam begins, you are granted five minutes to read the (ISC)^2 Non-Disclosure Agreement (NDA). If you fail to read and accept it within the allotted time, your exam will end, and you lose your exam fees! Instead of dealing with this kind of pressure right before answer 150 tough questions, I recommend you download and read the NDA before test day. You can find a link to download the NDA in Appendix B.

TIP

Some questions on your exam may appear to have multiple right answers, but success on the CCSP requires that you select the *best* answer for each question. Use the process of elimination to get rid of two answers that are clearly wrong. You'll be left with the correct answer and what *psychometricians* (people who study the science of testing) call a distractor. If you take a deep breath and dig deep into your memory bank, you'll have a great shot at eliminating the distractor and choosing the single correct answer.

Identifying What to Do After the Exam

After four grueling hours (or less) and 150 mind-bending questions, you're all done with your CCSP exam! So, now what? Well, in most cases, you'll have your unofficial test results as soon as you finish the exam — hopefully you've passed, and you can go celebrate!

If, for whatever reason, you don't pass the exam on your first try, don't fret! It's not uncommon for folks to need a couple tries on such a tough exam — although *CCSP For Dummies* is here to help you avoid that fate! Candidates who fail their first try must wait 30 days before taking the exam again. If failure happens to you, I strongly recommend you read this book again and take lots of practice exams within that 30 days. If you fail a second time, you must wait 90 days to try again.

If you fail again, I need you to eat, drink, and sleep cloud security for that 90 days! Read and reread this book (and review your other resources) until you know all six domains inside and out.

Okay, enough about that — you're here to pass the CCSP! Once you receive formal notification that you've passed the exam, you have nine months to complete the CCSP endorsement process. Endorsement is the act of having an existing (ISC)² credential holder attest to your work experience and give (ISC)² the thumbs-up to welcome you into the family. Visit `www.isc2.org/endorsement` for more information.

Once you pass the exam and complete the endorsement process, you are officially a Certified Cloud Security Professional! But this isn't the end of your journey — in fact, your CCSP journey is a lifelong one. You must remain a member in good standing by doing two things:

- **Paying your annual maintenance fee (AMF):** All (ISC)² certified members must pay an AMF of $125 every year on their certification anniversary (except those who hold only the CC certification — they pay $50 per year). (ISC)² uses members' AMFs to maintain their certifications and all the support systems and benefits that come with being a member.
- **Completing your Continuing Professional Education (CPE):** Once you're a CCSP credential holder, you must demonstrate ongoing maintenance and enhancement of your cloud security knowledge by earning CPEs. As a CCSP, you must earn at least 90 CPE credits every three years, with a suggested minimum of 30 CPEs annually. You can earn CPE credit by completing activities that are directly related to the CCSP domains, including (but not limited to)
  - Attending a conference, seminar, or presentation
  - Finishing a project that's outside your normal work duties
  - Writing a whitepaper or book
  - Volunteering for a charitable organization
  - Taking a higher education course
  - Reading a book or magazine