EXPERT REFERENCE SERIES OF WHITE PAPERS

CISSP Exam Changes - 2021 Study Guide

Global Knowledge®

CISSP Exam Changes - 2021 Study Guide

The 2021 revised and updated version CISSP (Certified Information System Security Practitioner) certification exam will be released on May 1, 2021. This new version of the popular CISSP exam will include a modest revision and re-organization of previously included topics, but will integrate a significant number of new topics. The test remains adaptive and preparing for the CISSP exam will be more challenging than ever before. You will need to be knowledgeable in all eight domains of CISSP in order to pass.

This paper discusses the importance of the CISSP certification, identifies the new 2021 exam version topics, reveals the complexity of the adaptive testing format, and provides guidance for your preparations towards successfully passing the CISSP exam.

The value of CISSP stands out in a crowded industry

Many certification roadmaps include CISSP as an important security certification to consider in a career and education plan. One example of this is the CompTIA IT Certification Roadmap, which places CISSP in the "Expert" column of the Information Security pathway. The CompTIA roadmap of IT certifications is not alone in recognizing the importance and value of this certification.

CISSP is a widely desired indicator of knowledge, experience, and excellence on the resume of many IT professionals. CISSP is not just a recommendation by industry groups—it has achieved its respected position as an important IT certification through practical observation. The drive to achieve this notable certification is evidenced in its appearance on a significant number of job postings. Performing a job search in any moderate or larger metropolitan area reveals that an astounding number of IT and security positions request that the applicant be CISSP-certified.

A quick scan of resume posting sites also shows that a number of IT professionals who are either currently employed or are job seeking include CISSP on their resume and/or profile in order to attract the attention of top job brokers and HR managers.

(ISC)^2 asserts there are over 142,000 CISSP-certified individuals located in order 170 countries worldwide, and that number is growing at a steady pace. Those who hold the CISSP certification are employed at Fortune 500 companies, governments, small businesses, start-ups, and many operate as independent contractors.

According to the Global Knowledge 2020 IT Skills and Salary Report, CISSP-certified professionals have the highest worldwide IT salaries ($119,170 USD) and rank fifth in the United States ($138,647 USD). CISSP is also listed as the second most common certification being pursued by IT professionals seeking to advance their career.

A 2020 salary survey by Certification Magazine reveals even further insights into the demographics of those holding the CISSP certification.

- Over 7% of surveyed certification holders are women
- 70% of CISSP holders are aged 35 to 54
- 41.7% have a master's degree and an additional 36.4% hold a bachelor's degree
- 96.8% are employed full-time
- CISSP holders are often senior specialists (43.2%), managers (16.7%), directors (14%), senior managers (13%), specialists (6.5%), or executives (3.4%)
- 72.1% have worked in cybersecurity for over a decade

[Note: Visit certmag.com for the full details on the survey and their methodologies. All percentages are derivative of those who responded to the survey and many not fully reflect the entire worldwide status of CISSP certification holders.]

Domain weighting changes

The domains are the groupings of topics defined and organized by (ISC)^2 based upon their survey of the cybersecurity industry (previously referred to by the term Common Body of Knowledge (CBK)) and their annual Cybersecurity Workforce Study (a.k.a. Job Task Analysis (JTA)). The CISSP exam has eight domains. The number and names of these domains are remaining consistent between the previous 2018 exam version and the 2021 exam version. The only domain-level changes are adjustments to the weighting of domain-focused questions where Domain 4 is reduced by one percent and Domain 8 is increased by one percent as seen in this table:

2018 CISSP Exam	2021 CISSP Exam
1. Security and Risk Management 15%	1. Security and Risk Management 15%
2. Asset Security 10%	2. Asset Security 10%
3. Security Architecture and Engineering 13%	3. Security Architecture and Engineering 13%
4. Communication and Network Security 14%	4. Communication and Network Security 13%
5. Identity and Access Management (IAM) 13%	5. Identity and Access Management (IAM) 13%
6. Security Assessment and Testing 12%	6. Security Assessment and Testing 12%
7. Security Operations 13%	7. Security Operations 13%
8. Software Development Security 10%	8. Software Development Security 11%

New topics to master

The 2021 revision to CISSP has many new topics listed on the Certification Exam Outline. Some of the items listed as new are topics that may have been covered or included in the 2018 CISSP exam, but they were not specifically mentioned on the 2018 Exam Outline. Here is a presentation of the new topics on the 2021 CISSP exam Certification Exam Outline:

Note: The domain topic numbering scheme used here is an extension of that found in the Certification Exam Outline. The first numeral is the primary domain and the second numeral is the sub-domain topic (often a longer phrase) these two numbers are used by (ISC)^2 in the Certification Exam Outline. A third numeral (if present) is an additional reference number added by me to indicate the sub-sub-topic which is from the bulleted list under a sub-domain topic. This numbering scheme allows for ease in locating the numbered-in-order bulleted topics from the Certification Exam Outline. All items listed in this section are new in 2021, some items have additional clarification statements.

Domain 1: Security and Risk Management

1.2.1 Confidentiality, integrity, availability, authenticity and nonrepudiation

[Authenticity is a newly listed item, nonrepudiation is new in Domain 1, it also still appears as non-repudiation in 3.6]

1.9.3 Onboarding, transfers, and termination processes

["transfers" is new in 2021]

1.10.6 Control assessments (security and privacy)

[Privacy control assessments is new, and this sub-sub-topic is renamed from 2018 1.9.6 "Security Control Assessment (SCA)"]

1.10.9 Continuous improvement (e.g., Risk maturity modeling)

["Risk maturity modeling" is new for 2021]

1.12 Apply Supply Chain Risk Management (SCRM) concepts

[SCRM is new in 2021]

1.13.1 Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

["social engineering, phishing, security champions, gamification" are all new topics in 2021]

Domain 2: Asset Security

2.3 Provision resources securely

2.3.2 Asset inventory (e.g., tangible, intangible)

["tangible, intangible" new in 2021]

2.4 Manage data lifecycle

2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)

2.4.2 Data collection

2.4.3 Data location

2.4.4 Data maintenance

2.4.5 Data retention

2.4.6 Data destruction

2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

["EOL" and "EOS" are new in 2021]

2.6.1 Data states (e.g., in use, in transit, at rest)

["in use, in transit, at rest" data states are new in 2021]

2.6.4 Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

[DLP and CASB new in 2021]

Domain 3: Security Architecture and Engineering

3.1.2 Least privilege
[new for 2021, but also present in 7.4.1]
3.1.3 Defense in depth
3.1.4 Secure defaults
3.1.5 Fail securely
3.1.7 Keep it simple
3.1.8 Zero Trust
3.1.9 Privacy by design
3.1.10 Trust but verify
3.1.11 Shared responsibility
3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
["Biba, Star Model, Bell-LaPadula" new in 2021]
3.5.6 Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
[SaaS, IaaS, and PaaS new in 2021]
3.5.9 Microservices
3.5.10 Containerization
3.5.11 Serverless
3.5.13 High-Performance Computing (HPC) systems
3.5.14 Edge computing systems
3.5.15 Virtualized systems
3.6.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
["quantum" new in 2021]
3.6.5 Digital signatures and digital certificates
["Digital certificates" new in 2021]
3.7.1 Brute force
3.7.2 Ciphertext only
3.7.3 Known plaintext
3.7.4 Frequency analysis
3.7.5 Chosen ciphertext
3.7.6 Implementation attacks
3.7.7 Side-channel
3.7.8 Fault injection
3.7.9 Timing
3.7.10 Man-in-the-Middle (MITM)
3.7.11 Pass the hash
3.7.12 Kerberos exploitation
3.7.13 Ransomware
3.9.9 Power (e.g., redundant, backup)

Domain 4: Communication and Network Security
4.1.2 Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
[IPSec, IPv4, and IPv6 new in 2021]
4.1.3 Secure protocols
4.1.5 Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
[FCoE, iSCSI, and VoIP new in 2021]

4.1.6 Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
[Micro-segmentation, VXLAN, encapsulation, and SD-WAN new in 2021]
4.1.7 Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
[Li-Fi, Zigbee, and satellite new in 2021]
4.1.8 Cellular networks (e.g., 4G, 5G)
4.2.1 Operation of hardware (e.g., redundant power, warranty, support)
4.3.6 Third-party connectivity

Domain 5: Identity and Access Management (IAM)
5.1.5 Applications
5.2.5 Registration, proofing, and establishment of identity
["Establishment of identity" new in 2021]
5.2.8 Single Sign-On (SSO)
5.8.9 Just-in-Time (JIT)
5.3.3 Hybrid
5.4.6 Risk-based access control
5.5.1 Account access review (e.g., user, system, service)
["service" new in 2021]
5.5.2 Provisioning and deprovisioning (e.g., on/off boarding and transfers)
["on /off boarding and transfers" new in 2021]
5.2.3 Role definition (e.g., people assigned to new roles)
5.2.4 Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
5.6 Implement authentication systems
5.6.1 OpenID Connect (OIDC)/Open Authorization (Oauth)
5.6.2 Security Assertion Markup Language (SAML)
5.6.3 Kerberos
5.6.4 Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Domain 6: Security Assessment and Testing
6.2.9 Breach attack simulations
6.2.10 Compliance checks
6.4.1 Remediation
6.4.2 Exception handling
6.4.3 Ethical disclosure

Domain 7: Security Operations
7.1.5 Artifacts (e.g., computer, network, mobile device)
7.2.5 Log management
7.2.6 Threat intelligence (e.g., threat feeds, threat hunting)
7.2.7 User and Entity Behavior Analytics (UEBA)
7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
7.7.1 Firewalls (e.g., next generation, web application, network)
["next generation, web application, network" new in 2021]
7.7.8 Machine learning and Artificial Intelligence (AI) based tools

7.11.7 Lessons learned

Domain 8: Software Development Security

8.1.1 Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps)
["Agile, Waterfall, DevOps, DevSecOps" are new in 2021]
8.1.2 Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
[CMM and SAMM are new in 2021]
8.2.1 Programming languages
8.2.2 Libraries
8.2.3 Tool sets
8.2.4 Integrated Development Environment (IDE)
8.2.5 Runtime
8.2.6 Continuous Integration and Continuous Delivery (CI/CD)
8.2.7 Security Orchestration, Automation, and Response (SOAR)
8.2.10 Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
8.4.1 Commercial-off-the-shelf (COTS)
8.4.2 Open source
8.4.3 Third-party
8.4.4 Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
8.5.4 Software-defined security

Upon close inspection you might recognize that some of these "new" topics are already covered or are reasonable expansions of the domains. Many of the "new" topics should be familiar to any current cybersecurity professional. Be sure to focus on these topics in your preparation as they may be slightly more prevalent in exam questions than "legacy" topics.
Note: Please refer to the full 2021 CISSP Certification Exam Outline for the complete current topic list.

The official Certification Exam Outline

The 2021 update to the CISSP exam introduces many new topics and revisions of topics present on the previous version of the exam. The official Certification Exam Outline is the primary source of what is included on this latest update of the CISSP exam. You can obtain your own copy of the Certification Exam Outline (which was previously known as the Candidate Information Bulletin or CIB) by visiting the CISSP section of the (ISC)^2's website (https://www.isc2.org/Certifications/CISSP) and scrolling down the page to the section titled "Your Pathway to Certification." Under this heading, click on the box labeled as "2| Register and Prepare for the Exam." This reveals the current list of domains and offers a download link for the Certification Exam Outline in various languages. Until May 1, 2021, this page will offer both the 2018 and the 2021 versions of the Exam Outline, so make your selection carefully. (Note: The first page of this PDF document shows the title as "Certification Exam Outline," but many mentions of this document on (ISC)^2's website uses the name "CISSP Exam Outline.")

The Certification Exam Outline, which is sometimes referred to as an objective's list, is the presentation of the range of topics that (ISC)^2 is including on the CISSP exam. It is organized into eight domains, which are sub-divided into numbered sub-objectives or sub-domain, which are in turn often divided into numerous bullet point items. This bullet items are defined by (ISC)^2 as examples. Also, several items on the Exam Outline include parenthetical lists of related topics. Everything listed on the Exam Outline is fair game as a topic of focus for an exam question. However, do not assume that the Exam Outline is exhaustive and complete. (ISC)^2 reserves the right to include related or similar topics on the exam that are not directly and specifically named in the Exam Outline.

What to know about the CISSP-CAT process

The legacy original CISSP exam was a paper-based, bubble-sheet test consisting of 250 questions to be completed in a six-hour time window. With the 2015 revision, the CISSP exam was available as a computer-based testing (CBT) option through Pearson VUE testing locations, but it retained the question count and time limit of its predecessor. With the 2018 revision, (ISC)^2 adopted the current CISSP-CAT mode of exam delivery.

The CISSP-CAT is the current mode or method of exam delivery employed by (ISC)^2 for the English version of the exam. CAT stands for Computer Adaptive Test. The CISSP-CAT only applies to the English version of the exam. For non-English versions, the 250-question, six-hour version is still used.

The CISSP-CAT format

You will view a minimum of 100 questions and a maximum of 150 with a three-hour time limit. Of the first 100 questions, only 75 are graded and count towards your score. The 25 ungraded questions are not marked, and are interspersed throughout the first 100 questions. These questions are used to evaluate questions for future tests. Rather than working towards accumulating points to cross a line to pass, (ISC)^2 evaluates your ability to demonstrate knowledge in relation to a concept called the passing standard. (ISC)^2 does not publicly define what the level of achievement is to surpass the passing standard. However, it is most likely scoring 70% or greater within each of the eight domains.

At question 100, the system evaluates your potential to achieve the passing standard. If the system estimates your pass potential is 95% or higher, the test will end with a pass. If the system estimates your failure potential is 95% or higher, the test will end with a fail result. If a 95%+ pass/fail determination cannot be made at question 100, then it is evaluated again after each question until you reach question 150. You are only assessed on the last 75 graded questions. This means that as you answer question 101, the first graded question is discarded and replaced with question 101. Then as you answer question 102, the second originally graded question is discarded and replaced with question 102, and so forth. As a question is “dropped” from being considered towards your pass/fail potential, it is replaced by a question of the same domain. This is how the exam maintains the domain coverage percentages.

Don’t skip questions

You get one chance to view a question and provide an answer. You cannot revisit previous questions. Although it is not stated, a skipped question is likely marked as incorrect. Therefore, guessing is still a better strategy than skipping. You should always attempt to eliminate question options from consideration, then select your answer from the remaining options.

In early 2021, (ISC)^2 announced that they are performing a pilot test for performing the CISSP exam through an online remote proctoring system. (ISC)^2 has remained one of last major certification entities that had not adopted a remote examination and online proctoring process for taking their certification exams. Based on the results of their preliminary pilot program which will occur in Feb 2021, (ISC)^2 may elect to offer online remote proctored testing for CISSP and other (ISC)^2 certs in the future. The statements released by (ISC)^2 about the program indicate that the remote online exam will be a linear (i.e., not adaptive) 250 question six-hour exam, and you will not be able to revisit questions once an answer is submitted. For more information on this, visit the (ISC)^2 blog and other relevant links:

- https://blog.isc2.org/isc2_blog/
- https://www.isc2.org/Exams/online-proctor-pilot-test-FAQ
- https://www.isc2.org/News-and-Events/Press-Room?

CISSP exam tips and tricks

The 2021 CISSP exam questions seem to have the same level of depth and complexity as previous versions, with only a handful of new topics. The CISSP-CAT testing method or structure itself is often the most daunting part of achieving the certification for those who sit the exam.

(ISC)^2 claims that the assessment of a candidate’s knowledge and mastery of relevant topics is equivalent between the CISSP-CAT and the traditional flat version of the exam. However, I think there is an increased requirement to be knowledgeable across all eight domains rather than only needing to be proficient in six on the traditional flat or linear version. On legacy linear versions, you needed to answer enough questions correctly to accumulate a score above the minimum to pass. This seemed to allow a tester to score poorly in two domains, while scoring well in the other six and still be able to achieve a passing score. The CISSP-CAT testing mode evaluates the tester in all eight domains and in order to pass you much achieve the “passing standard” in each domain.

Some training and exam preparation guidance for previous versions of the exam seem to indicate that you could overlook or ignore one or two domains that you found overly challenging and focus on the six domains that were more comfortable to the test taker. I don't think this is now a valid and responsible strategy for passing the CISSP exam. Therefore, you may need to spend additional time studying and preparing for the CISSP exam to ensure you are well-versed in most topics across all eight domains.

Here are my recommendations for CISSP exam prep:

- Use the 2021 Certification Exam Outline as a guide to make sure you comprehend every topical statement and bulleted item.
- Develop a set of personal flash cards for topics that you find challenging to keep front-of-mind. Work through your flash card set multiple times per day until you master each element.
- Find and use practice question sets (see the last section for help). As you complete your studies for a domain, take 100 or more practice question for that specific domain. Work on scoring 80% or better per domain.
- Once you have "completed" your studies, find and take full length practice tests (125-150 questions each) that cover topics across domains. Work on scoring 80% or better on these.
- For each question you get incorrect, spend time researching and studying the right answer and understand the wrong answer that distracted you. You will only improve your knowledge by focusing on what you don't know or are getting incorrect.

Four studying basics

For most of us, we never were really taught how to study. As a careered professional, it is often assumed you know how to study. Here are the basics:

1. Don't cram. Your mind does not absorb and retain lots of new content quickly or easily. You need to spread your studying over time.
2. Don't spend more than 30 minutes in a single sitting. Use the Pomodoro Technique by setting a timer for 25 minutes, do ONLY study tasks for 25 minutes, then give yourself a timed five-minute break. A break is an absolute must; it needs to be something COMPLETELY different from your study activities, so make it an active moving break that is a solid distraction from the study materials. Repeat up to four times before having a 30-minute break.
3. Break up materials into reasonably-sized chunks or sections. This could be a domain or sub-domain division, chapter of a study guide, or blocks of practice questions.
4. Focus on what you don't know and on the practice questions you get wrong.

For many, studying for CISSP may take an additional 4-6 weeks after a training course or 8-12 weeks solely of self-study.

Test-taking skills

Some of the skills needed to pass the exam are knowing the topics related to CISSP while others are test-taking skills. Here are some important concepts to keep in mind:

- Look for relationships between answer options. For single answer multiple choice, if two answers are synonyms, then neither can be the correct answer.
- Sometimes a question wants a detailed answer, while others a generic or broad answer.
- Some answer options are related in a parent-child or super-set/sub-set relationship. Recognizing this may help resolve some questions.
- Watch out for negative statements, such as not or never, these can inverse the focus of the question.
- Look for absolutes and realize there are few absolutes in security.
- Think like a manager. Your goal is to protect the ability to perform business objectives, to complete business missions and goals, and to do so while minimizing downtime, avoiding legal consequence, and optimizing return on security investment (RoSI).
- Some questions are written using ambiguous language or loose grammar. Read the question stem, then the answer options, then re-read the question stem before attempting to select an answer.
- Always evaluate the question considering the CIA triad.
- Some questions may include non-existent, obtuse, or esoteric answer options, if you don’t recognize something (and you studied thoroughly), consider it a wrong answer.
- Determine if a question is asking for an example (i.e., how) or a definition (i.e., what).
- Always write out math issues on your scratch pad.
- Eliminate answer options from consideration which are obviously incorrect. Select your beset answer from the remaining options.
- Look out for flip-flop or waffling answer options, items that are sometimes true and also sometimes false are typically wrong answers.
- Don’t rely upon only your own experience, if you work in the government and military, then reconsider answers in light of private sector business and vice versa.
- The goal of security is not 100% maximum security, but sufficient security for the organization’s risk tolerance.
- Think of yourself as a risk advisor rather than a problem solver.
- Think more about the why security should be done rather than the how it is accomplished.

How to get certified and remain certified

The CISSP certification is designed for experienced IT professionals. To fully achieve the certification, you need to have five years of cumulative paid relevant work experience in two or more of the CISSP topical domains. There are some options of substituting one year of experience for a recent IT or security-related college degree or another authorized certification from a list of over 50 qualifying options.

Your experience will be confirmed by another person holding CISSP in good standing. This process is called endorsement. You have nine months after passing your exam to complete the endorsement process and achieve the CISSP certification. If you fail to be endorsed by that deadline, you lose your exam passing status and will have to re-take the exam.

If you don't have five years of relevant experience, you can still take the CISSP exam, and then you'll have up to six years to obtain or finish obtaining the five years of required experience. This pathway to certification is known as the "Associate of (ISC)^2." It means you will take the same CISSP exam, but the endorsement deadline is extended to six years. During your exam registration, one of the last questions you are asked is about whether or not you are pursuing the "Associate of (ISC)^2." If you are unsure about your experience, select the "Associate of (ISC)^2" path. There is no requirement to wait six years to complete the endorsement, and you can still perform it the week after you pass the exam if you do have five years of relevant experience.

Do not claim to be CISSP-certified in conversations, in email, or on your resume until you have received the welcome packet from (ISC)^2. You will receive the welcome packet after you have met all the requirements and your endorsement is accepted. This welcome packet will arrive by postal mail and will include a certificate of achievement suitable for framing along with instructions for how to take advantage of the many benefits of being CISSP certified.

Take the (ISC)^2 Code of Ethics seriously. If you are found to be in violation of the Code of Ethics, (ISC)^2 can strip you of your certification and bar you from ever taking one of their certifications again. As long as you are an ethical and law-abiding individual, this should not be a concern.

Continuing professional education credits

Every three years you must earn 120 continuing professional education (CPE) credits to maintain your CISSP certification. Details about CPEs are also available in the (ISC)2 Continuing Professional Education (CPE) Handbook. Additionally, you will have the privilege of paying an Annual Maintenance Fee (AMF) of $125 for your CISSP certification. Your first AMF is due immediately upon achieving certification, then it is due each year on your anniversary date (typically your endorsement completion date). The details regarding AMFs are available in the (ISC)^2 Member Policies Portal in the section "(ISC)^2 Certification and Membership Maintenance Policy" under heading "4.2 Annual Membership Fee (AMF) Requirement". Once certified, you will have access to the members-only area of the isc2.org web site where you can keep track of your earned CPEs and pay your AMFs. Failing to meet either requirement will result in the suspension of the certification and if not resolved within two years, termination of the certification.

How to prepare for the CISSP exam

In order to prepare for the CISSP exam, there are several resources or paths to consider.

Instructor-led training

I highly recommend attending a CISSP preparation training class. Global Knowledge offers a CISSP Certification Prep Course that provides in-depth coverage of all eight domains required to pass the CISSP exam.

Instructor-led classroom or virtual classroom courses will immerse you in the concepts and details of CISSP material. A training course will focus your attention on CISSP for the duration of the class and give you the opportunity to interact with other students and the instructor to gain a deeper understanding of topics, as well provide an opportunity to get your questions answered.

Self-study

Another preparation path is self-study. For some who already possess strong core skills in the area, this may be a enough to prepare for the CISSP exam. However, I would recommend assessing your abilities and knowledge base early. In the event you are not able to obtain the knowledge on your own, plan on attending a formal training class. To assess your preparedness, you need to use a 100- to 150-question practice exam that covers the full range of CISSP topics. If you score 80% or better, then you are likely able to self-study for the exam.

Resources

Even if you are taking an instructor-led prep course, self-study should complement it. Either way, there are several resources I recommend. A good study guide is always an excellent starting point. The *CISSP Study Guide 9th Edition* (https://amzn.to/38EomK5) is a great choice. It is the book used by Global Knowledge in their CISSP training classes, and I am one of its three authors. It includes coverage of every topic listed on the official Certification Exam Outline, plus other subjects that support the main topics, relate to the main topics, or that round out your knowledge and understanding of the main topics. This book includes end-of-chapter questions which are also available online through a testing engine. The online resources include the end-of-chapter questions plus an additional 500 questions grouped as four 125-question practice tests that do not appear in the book, as well as a large glossary and over 1,000 flash cards.

For additional practice questions, I recommend the following:

- The CISSP Official Practice Tests 3rd edition (https://amzn.to/2XF3kEW)
- The quiz engine at skillset.com
- The quiz engine at cccure.education
- The practice questions from Boson

However you elect to study, be sure to regularly review the Certification Exam Outline to make sure that you fully understand every listed item. You also want to round out your preparation by taking numerous full length (100 –150 question) practice tests and seek to consistently achieve 80% correct. This should indicate that you are well prepared to take and pass the CISSP exam. I'm sure that with some directed study and being armed with the information from this paper, you are sure to be able to successfully pass the 2021 revision of the CISSP exam. The CISSP certification is a solid addition to your resume, it may earn you the respect of your peers, and it may expand your wallet.

I wish you diligent studies and a successful attempt at the CISSP certification exam.

Related course

- CISSP Certification Prep Course
- GK Polaris Discovery
    - Includes the CISSP prep course and other cyber courses

Related papers

- CISSP has Changed Again; What it Means for your Certification Prep
- Everything You Need to Know About the 2021 CISSP Exam Changes

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses for over 25 years, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He has taught hundreds of classes accumulating over 20,000 hours of instruction. He is the author of and contributor to more than 80 books on security and certifications. His most recent publications include the *CISSP Study Guide 9thth Edition* and *Security+ Review Guide 5th Edition (SY0-601)*. Michael has also contributed to many other security focused materials including exam preparation guides, practice exams, video instruction, and courseware. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds variety of certifications, including: CEH, CHFI, ECSA, ECIH, CND, CEI, CASP+, CySA+, PenTest+, Security+, Network+, A+, CTT+, CISSP, CISM, and CFR. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. Michael is an independent contractor (i.e., a cybersecurity mercenary) who is available to provide training for your personnel or for the crafting of custom content. You can reach Michael by e-mail at michael@impactonline.com or visiting impactonline.com.