INFOSECTRAIN

Phone : +91-97736-67874
Email : sales@infosectrain.com
Web : www.infosectrain.com

HOW TO PREPARE FOR INFOSEC DOMAIN'S BEST CERTIFICATIONS?

Introduction

Information security and certifications go hand in hand. Information security domain's certifications play a huge role in career choices and successes today. Some of the prominent Information security certifications are the CISSP, CCSP, CISM, CISA, CEH, CRISC. This paper lays out the way in which we can prepare for industry's most coveted certifications.

Why Choose Us

- ☑ Learn from Industry Experts
- ☑ 24X7 Post Support
- ☑ Certification Focused Programs

CISSP® CCSP™ CISA® CISM® CRISC

1. How to prepare for CISSP?

Here are the details about how to prepare for the most coveted exam in the Information security domain:

1.a. Exam Details:

1. A CISSP candidate must demonstrate a minimum of **5 years** of full-time security experience in two of the eight domains of the (ISC)^2 CISSP CBK(Common body of knowledge)
2. The candidate must score **700 out of a possible 1000 points** to pass the exam
3. The duration of the exam is about **3 hrs**.
4. All English versions of the CISSP exam use CAT or 'Computerized adaptive testing'
5. The candidate can check the pricing of the exam from this link
6. The exam has about **100-150 questions**

1.b Exam Tips:

1. Book a date for the exam at least **3 months** away and start studying immediately
2. It is good to study for at least 4 hours every day
3. It is necessary to draw a timetable and stick to it diligently
4. It is also necessary to take into account the different personal and official responsibilities in the three-month time frame and adjust the timetable and work hours accordingly
5. Since the exam has 100-150 questions which have to answered in 180 minutes the candidate needs to be totally thorough with all the topics of the exam. Since there is a chance that the questions will be wordy, you need to have an absolute grasp over all the topics of the exam.
6. Patience, persistence, and consistency are some factors that will help you to crack the exam

These exam tips are common for all exams.

1.c. Resources:

- Official (ISC)^2 Guide to the CISSP CBK ((ISC)2 Press) 4th Edition by Adam Gordon

- This official (ISC)^2 book contains enhancements to the CISSP syllabus and it was published in 2015. This new book contains the modified and current CISSP eight domains and questions pertaining to them.

- The Official (ISC)2 Guide to the CISSP CBK Reference 5th Edition, Kindle Edition by John Warsinske (Author), Mark Graff (Contributor), Kevin Henry (Contributor), Christopher Hoover (Contributor), Ben Malisow (Contributor), Sean Murphy (Contributor), Charles Oakes (Contributor), George Pajari (Contributor)
- This CBK covers the new eight domains of CISSP with the necessary depth to apply them to the daily practice of information security. Written by a team of subject matter experts, this comprehensive reference covers all of the more than 300 CISSP objectives and sub-objectives in a structured format with:

  - ✓ Common and good practices for each objective
  - ✓ Common vocabulary and definitions
  - ✓ References to widely accepted computing standards
  - ✓ Highlights of successful approaches through case studies
- (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide 8th Edition by Mike Chapple (Author), James Michael Stewart (Author), Darril Gibson (Author)
- This Sybex study guide has expert content, real-world examples, advice on passing each section of the exam and access to the Sybex online interactive learning environment.
- CISSP Official (ISC)2 Practice Tests 2nd Edition
- These are the official practice tests available from (ISC)^2. These practice tests are aligned with the latest version of the CISSP exam. This book contains 1300 unique practice questions. In addition, the first part of the book alone contains 100 questions per domain.
- Eleventh Hour CISSP®: Study Guide 3rd Edition
- The 'Eleventh Hour CISSP' is tuned to the current syllabus of CISSP and is streamlined to include core certification information and it is primarily used for last minute studying.
- NIST publications
- The following list details the various publications that a candidate should be well-versed in to pass the CISSP exam.

  - ✓ SP 800-12 - An Introduction to Computer Security
  - ✓ SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
  - ✓ SP 800-30 - Risk Management Guide for Information Technology Systems
  - ✓ SP 800-34 - Contingency Planning Guide for Information Technology Systems

- ✓ SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- ✓ SP 800-88 - Guidelines for Media Sanitization
- ✓ SP 800-137 - Information Security Continuous Monitoring

  SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organization
- ✓ SP 800-145 - The NIST Definition of Cloud Computing

1. d. Endorsement process:

All candidates who pass the exam must complete the endorsement process within 9 months. The application must be endorsed and digitally signed by an $(ISC)^2$ professional. The endorser must attest to the candidate's work experience in the IT security industry.

Once the candidate receives his CISSP credential from $(ISC)^2$, a candidate should recertify every 3 years.

1.e. Maintaining the certification:

Recertification is done by earning CPEs or 'Continuing professional education' and paying AMF (annual maintenance fees) of 85$. CPEs can be earned by joining webinars, attending events, reading and writing about Information security articles and books or volunteering.

2. How to prepare for CCSP:

Here are the details on how to prepare for the CCSP exam:

2.a Exam details:

1. Candidates for the CCSP exam must demonstrate at **least 5 years** of full-time work experience out of which **3 years** must be in the field of Information security and 1 year must be in one of **6 domains** of the CCSP exam.
2. The candidate must score **700 out of a possible 1000 points to pass** the exam
3. The duration of the exam is **4 hrs.**
4. The candidate can check the pricing of the exam from this link
5. The exam has about **125 questions**

2.b Resources:

The CCSP candidate should thoroughly know all the fundamentals related to encryption, virtualization technologies and the difference between IaaS, PaaS, and SaaS.

The candidate is expected to study the following books thoroughly in order to pass the exam with ease!

1. **The Official (ISC)^2 Guide to the CCSP CBK 2nd Edition, Kindle Edition** by **Adam Gordon**

   This is the first book that has to be studied and this is the (ISC)^2 endorsed study guide for the CCSP exam from Sybex. As organizations increasingly move their data to the cloud, cloud security assumes enormous significance in today's world. This second edition features clearer diagrams, real-life scenarios, illustrated examples, tables, best practices, and more.

2. Next, we recommend you to read the following pdf file from Cloud security Alliance which can be freely downloaded from this link:

   Security Guidance for critical Areas of focus in cloud computing v4.0

   The fourth version of the 'Security guidance for critical areas of focus in cloud computing' incorporates advances in cloud, security, and supporting technologies; reflects on real-world cloud security practices; integrates the latest Cloud Security Alliance research projects; and offers guidance for related technologies.

3. CCSP candidates should also read the 'The Treacherous 12' which is a freely downloadable file from CSA
   'Treacherous 12' are the top security threats that organizations face and this can be downloaded from the above link. Candidates are expected to read this before appearing for the CCSP exam.

4. Next, the candidates are also expected to download and read the CSA - Cloud Control Matrix
   The Cloud Control Matrix is used to provide guidance to prospective vendors and cloud customers in assessing the overall security risk of a cloud provider.

5. CCSP candidates are also expected to read the Jericho - Cloud Cube Model
   The Jericho cloud cube model differentiates the different cloud formations by the following factors:

   a. Internal/External
   b. Proprietary/Open
   c. Perimeterised/De-perimeterized Architectures
   d. Insourced/Outsourced

6. The candidate is also expected to know the ' OWASP top 10'
   OWASP is 'Open web application security project' is an open community that enables organizations to work with applications that can be trusted. They list the ten most critical web application security risks. Some of the risks last updated for the year 2017 are injection, broken authentication, 'sensitive data exposure' among others.

7. The candidate is also expected to read and familiarize themselves with the following NIST publications:
   a. NIST SP 800-146 Cloud Computing Synopsis and Recommendations
   b. NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
   c. NIST SP 800-125 Guide to Security for Full Virtualization Technologies

8. Finally, the candidate can download the electronic CCSP flash cards from $(ISC)^2$.
   This is a study tool for those preparing to take the CCSP exam. It is a unique and interactive way to test one's knowledge of industry terms and the various CCSP

domains.

This study tool can also be accessed via the phone both for Android and iOS via the Quizlet app.

9. Once you have studied from the various resources, the next step would be to test your knowledge of the CCSP exam before the big day. You can test your knowledge from these sources:

CCSP Official (ISC)2 Practice Tests 1st Edition
CCSP Certified Cloud Security Professional Practice Exams 1st Edition

'Cloud computing' being a rapidly changing field, it is also good to listen to various podcasts to keep up with the current trends.

Preparing for CCSP?

ENROLL NOW

3. How to prepare for CISA:

'CISA' is 'Certified Information Systems Auditor (**CISA**) refers to a designation issued by the Information Systems Audit and Control Association (ISACA) The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals.

Before we see how to prepare for CISA, here are few facts about CISA:

- ✓ As of 2017, 129,000 professionals have obtained the CISA certification which was introduced in 1978
- ✓ More than 94% OF PROFESSIONALS retained their CISA certification from the previous year(for the measured period)

3.a. Exam details:

1. A minimum **of 5 years** of professional information systems auditing, control or security work experience is required for certification. Waivers for experience can be obtained and more information can be viewed by following this link.
2. The exam is for a duration of **4 hours**
3. The registration fees for the exam, differs for ISACA members and non-ISACA members.
   ISACA members: US $575
   Non-ISACA members: US $760
4. The certification exam consists of **150 multiple choice** from the various job practice areas
5. ISACA uses a **200-800 point scale with 450** as the passing mark for the exams. A scaled score is a conversion of the raw score on an exam to a common scale. It is important to note that the exam score is not based on an arithmetic or percent average. A candidate must receive a scaled score of 450 or higher to pass the exam.

3.b. Resources:

- ❖ CISA Review Manual, 27th edition
  - ✓ This is a comprehensive reference guide designed to help individuals prepare for the CISA exam and understand the roles and responsibilities of an information systems (IS) auditor.
- ❖ CISA Review Questions, Answers & Explanations Manual 11th Edition
- ❖ This consists of 1,000 multiple-choice study questions. These questions are not

actual exam items but provide the candidates with the type of questions that had appeared previously in the exam.

- ❖ CISA Review Questions, Answers & Explanations Database—
  - ✓ This is a comprehensive 1,000-question pool of items that contains the questions from the CISA Review Questions, Answers & Explanations Manual 11th Edition. It is available online as well.
- ❖ CISA Online Review Course—
  - ✓ This course prepares learners to pass the CISA certification exam using proven instructional design techniques and interactive activities. You can either navigate the course through the recommended way or focus on more job practice areas.
- ❖ On-site CISA Exam Review Course
  - ✓ This course provides the learner the opportunity to study with an experienced, accredited professional. This may also include instructor led breakdowns of the five domains, mock exams and discussion forums.

3.c Maintaining the certification

1. Candidates who pass the CISA exam must maintain their certification by continuously earning CPEs or 'Continuous Professional education' over an annual and 3 year certification period. This enables the candidates keep up with the changes and maintain and upgrade their skills.
2. Successful candidates must report 20 CPE hours annually and 120 hours for a three year period.
3. Candidates can earn CPEs by attending webinars and virtual conferences, training courses, serving as an ISACA volunteer, mentoring.
4. Candidates must also pay the annual maintenance fees to ISACA headquarters. Refer this link for current rates.

Preparing for CISA?

ENROLL NOW

4. How to prepare for CRISC:

CRISC(Certified in Risk and Information Systems Control) certification is designed for those experienced in the management of IT risk, and the design, implementation, monitoring and maintenance of IS controls.
CRISC exam candidates should have a solid understanding of CRISC terminology and concepts. The CRISC exam will primarily align with the terminology and concepts described in ***The Risk IT Framework*, *The Risk IT Practitioner Guide***, and ***COBIT 4.1.***

Before we get started on how to prepare for CRISC exam, let us view the exam details.

4.1 Exam details:

1. Eligibility requirements: The candidate is expected to have three (3) or more years of experience in IT risk management and IS control. There are no substitutions or experience waivers.
2. The exam consist of **150 multiple choice questions** that cover the respective job practice areas created from the most recent job practice analysis.
3. Candidates have up to **4 hours (240 minutes)** to complete the exam.
4. ISACA uses a **200-800 point scale with 450** as the passing mark for the exams. A scaled score is a conversion of the raw score on an exam to a common scale. It is important to note that the exam score is not based on an arithmetic or percent average. A candidate must receive a scaled score of 450 or higher to pass the exam.
5. The registration fees for the exam, differs for ISACA members and non-ISACA members.
   ISACA members: US $575
   Non-ISACA members: US $760
6. There are four domains in the exam - IT Risk Identification (27%), IT Risk Assessment (28%), Risk Response and Mitigation (23%), Risk and Control Monitoring and Reporting (22%)

4.2 Resources:

It is good to obtain the resources listed below to ace the exam in the first attempt.

1. **CRISC Review Manual, 6th edition**
   The *CRISC Review Manual 6th Edition* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities.

The 6th edition manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- ✓ IT Risk Identification
- ✓ IT Risk Assessment
- ✓ Risk Response and Mitigation
- ✓ Risk and Control Monitoring and Reporting

2. **CRISC Review Questions, Answers and Explanations Manual 5th Edition by ISACA**

The *CRISC Review Questions, Answers & Explanations Manual, 5th Edition* is the study aid that is designed to familiarize candidates with the question types and topics featured in the CRISC exam with the use of 550 questions.

3. **CRISC Review Questions, Answers & Explanations Database - 12 Month Subscription by ISACA**

The *CRISC Practice Question Database is a comprehensive* 550-question pool of items that contains the questions from the *CRISC Review Questions, Answers & Explanations Manual 5th Edition*. The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity.

The complete set of resources can be found here.

4.3 Applying for the certification

Once you have passed your exam, the final step is to submit the CRISC application.

Prior to submitting the application you have to fulfill the following requirements:

- ✓ Pass the CRISC Exam within the last 5 years.
- ✓ Have the relevant full-time work experience in the CRISC Job Practice Areas
- ✓ Submit the CRISC Certification Application including application processing fee of US $50
- ✓ Adhere to the code of Professional Ethics

4.4 Maintaining the certification

In order to become and remain a CRISC an individual must agree to comply with the CRISC continuing professional education program. This program requires an individual to earn a minimum of 20 CPE hours annually and 120 CPE hours over the 3 year cycle years. In addition, an annual maintenance fee of US $45 ISACA member and US $85 non-member is required.

Preparing for CRISC? **ENROLL NOW**

5. How to prepare for CISM:

CISM (Certified Information Security Manager) is a management-focused certification. It promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security.

5.1 Exam details:

1. Eligibility requirements: Five (5) or more years of experience in information security management is required to take CISM. However, experience waivers are available for a maximum of two (2) years.
2. The CISM certification exam **has 150 multiple choice questions** from different job practice areas
3. The exam, is for a duration of **4 hours**
4. ISACA uses a **200-800 point scale with 450** as the passing mark for the exams. A scaled score is a conversion of the raw score on an exam to a common scale. It is important to note that the exam score is not based on an arithmetic or percent average. A candidate must receive a scaled score of 450 or higher to pass the exam.
5. Exam registration fees are based on membership status at the time of exam registration.
   ISACA Member: US $575
   ISACA Nonmember: US $760

6 The different domains are – Information Security Governance (24%), Information Risk Management (30%) , Information Security Program Development and Management (27%), Information Security Incident Management (19%)

5.2 Resources:

The following is a list of resources that can be used to pass the exam.

1. CISM Review Manual, 15th edition

The *CISM Review Manual 15th Edition* is designed to helps the candidate prepare for the CISM® exam. This comprehensive, easy-to-navigate manual is organized into chapters that correspond to the four job practice areas covered in the CISM exam. The manual is primarily designed as a tool for exam prep, but can also be useful as a reference manual for information security managers.

2. **CISM Review Questions, Answers & Explanations, 9th Edition by ISACA**
   The *CISM Review Questions, Answers & Explanations Manual 9th Edition* consists

of 1,000 multiple-choice study questions, answers and explanations, which are organized according to the CISM job practice domains.

3. **CISM Review Questions, Answers & Explanations Database • 12 Month Subscription**

   The CISM® Review Questions, answers & explanations database is a comprehensive 1000-question pool of items that contains the questions from the CISM® Review Questions, Answers & Explanations Manual 9th Edition. The database is available via the web, allowing the CISM candidates to log in at home, at work or any place that has Internet connectivity. The database is MAC and Windows compatible.

   The complete set of resources that can be used to study for the CISM exam can be found here

5.3. Applying for the certification:

Once you have successfully passed the CISM exam, you have to apply for the certification to complete the process. Before you apply, here are a few requirements that have to be met:

- ❖ You should have passed the CISM Exam within the last 5 years.
- ❖ You should have the relevant full-time work experience in the CISM Job Practice Areas.
- ❖ You should submit the CISM Certification Application including Application Processing Fee of US $50

5.4. Maintaining the certification

In order to become and remain a CISM an individual must agree to comply with the CISM continuing professional education policy. This policy requires an individual to earn a minimum of twenty (20) continuing professional education hours annually and one hundred and twenty (120) continuing professional education hours for every three year cycle. In addition, an annual maintenance fee of US $45 ISACA member and US $80 nonmember is required.

Preparing for CISM?

ENROLL NOW

AUTHOR

Jayanthi Manikandan (in)

Writer And Editor

“ Jayanthi Manikandan has a Master’s degree in Information systems with a specialization in Information Assurance from Walsh college, Detroit, MI. She is passionate about Information security and has been writing about it for the past 6 years. She is currently ‘Security researcher at InfoSec train. “

REVIEW BY

Prabh Nair (in)

Information security consultant

“ Prabh Nair has spent long years in the Information security sector, working on various short-term assignments for more than a hundred organizations across the globe in more than twenty countries. His work experience boasts of specializations in domains ranging from application security, vulnerability assessment, penetration testing, security solutions in governance to risk and compliance. Being a learner at heart, Prabh has always been keen to the idea of giving something back to the world, a desire which leads him to be an author and an Instructor to many I.T professionals. “