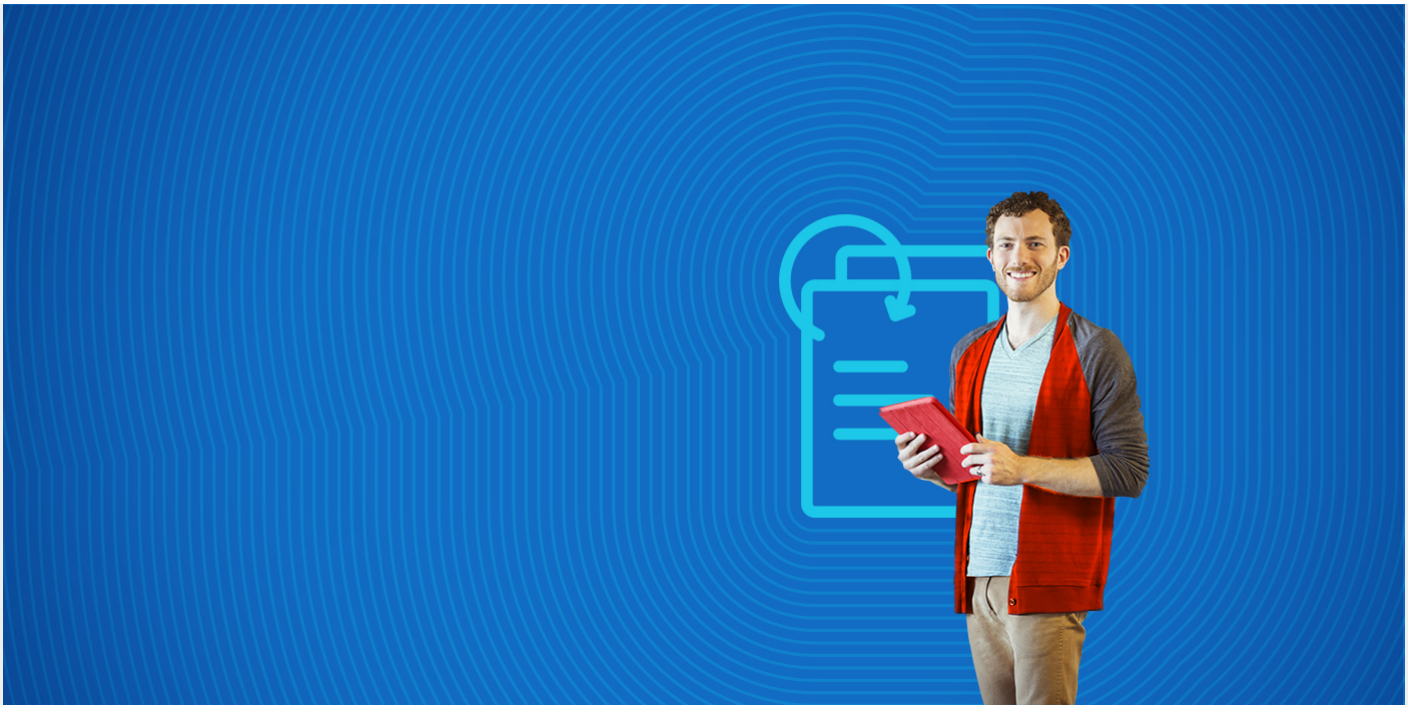
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP): AN INTRODUCTION



In any and every industry, becoming a top-ranked professional within a field requires reaching objectives like a certain number of years worked, elite training, and commitment to continuously learn new skills. As professionals advance in their careers, gaining globally recognized certifications that prove capabilities, as well as the three above mentioned objectives, will provide a reference for individuals, peers, and employers to measure competence and achievements.

For System Security professionals, one of the most coveted certifications is CISSP. In this article, we will discuss the ins and outs of this certification, skills covered in the examination process, prepping for the exam, and the advantages of hiring a CISSP employee.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

What Is CISSP and Who Is It For?

As countless businesses move operations online and the use of technology expands, the need for highly skilled professionals in the systems security industry is growing. As a matter of fact, protecting classified information that is stored digitally from cyberattacks or technology breaches is one of the hottest global topics these days.

And, with that, as information system security professionals are the first line of defense, according to Business News Daily, in 2018 North America was lacking 500,000 security professionals with a projection of that number reaching 4 million by 2021. To top it off, more than 10,000 positions in the US are available daily asking for CISSP hires.

Defined by Wedopedia as "a vendor-neutral certification reflecting the qualifications of information security professionals with an objective measurement of competence as well as a globally recognized standard of achievement. CISSP certification means the information security professional demonstrates a working knowledge of information security, confirms commitment to the profession, and establishes a standard of best practices." Essentially, this certification assures that an employee is qualified to protect even the most sensitive systems.

Established in 1989, this certification is backed by (ISC)2 and is recognized as the global standard for Information Systems Security excellence. It is an ideal certification for Chief Information Security Officers, Director of Security, IT Director/Manager, Security Systems Engineers, Security Analysts, Security Auditors, and more. However, keep in mind, it is not for everyone. For those in Cloud Security, IT/ICT Security Administration, Security Assessment, Secure Software Development, and Healthcare Security, there are other certification options available.

Why Hire A CISSP Employee?

A certification not for the faint of heart, the CISSP, as explained by Simplilearn is for "recipients are part of a pretty exclusive club. Only 94,000 professionals hold the CISSP certification worldwide (149 countries). The exam itself has an 80% failure rate." Those that hold this certification are dedicated, seasoned individuals that meet rigorous requirements and have extensive knowledge in the field.

The advantage of hiring this type of employee and paying the average yearly salary of 100K is significant. From better risk management to organization reputation improvement and higher quality standards, with a CISSP employee on the team, clients are more likely to work with a business, employees are exposed to more knowledge, and insurance demands are easily met.

The 5 Requirements

Beyond passing the in-depth examination and proving knowledge within all domains, the CISSP certification also requires the individual to have five years of full-time work experience in two of the eight domains. However, if the candidate has a 4-year degree, they may qualify for a 1-year waiver that reduces the work experience to four years. The exam may be taken any time, if passed before meeting the work experience requirements, the individual may become an associate of (ISC)2 and apply for certification after full-time employment. After six years have lapsed and work requirements are not met, the exam must be retaken. Once passing and proving full-time work history, the individual must agree to the organizational code of ethics, become endorsed, pass a background qualification, and recertify every three years.

To recap, the five requirements are:

1. **Real-World Work Experience (5 years or 4-year degree + 4 years)**

This work must be paid, full-time, and be within the fields of Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

2. **A score of 700 out of 1,000 on the CISSP exam**

Candidates are given six hours to complete the multichoice and innovative questions. The exam

itself costs $699 USD, but it is advised to take prep classes that cost anywhere from free to $3K. Obtaining third party study assistance is highly suggested.

3. **Background Qualifications**

According to the (ISC)2 website, it is expected that "certified members be of the highest ethical and professional caliber. To that end, the organization has standards that candidates must acknowledge as part of the certification criteria." Before sitting for the exam everyone must carefully answer questions, such as have you ever been involved with hacking, do you have an alias, has a professional license ever been revoked, as well as others.

4. **Agreement to code of Ethics and endorsement process**

After passing the work and exam requirements, the individual must acknowledge that this high level of guidance is not to be taken lightly. Professionals with this certification agree to uphold the safety, welfare, and common good of society. Among many other agreements, within the code of ethics, they honorably vow to advance and protect the profession. On top of that, another CISSP must endorse the candidate's work experience.

5. **Candidates must maintain certification every 3 years**

As stated above, this certification is not for the faint of heart Information Systems Security Professional. Once tackling the above four requirements, the certification must be maintained. At a cost of $85 USD every year, certified professionals must complete 40 continuing professional education credits yearly for a total of 120 every three years.

8 Examination Domains

After understanding the requirements and deciding to go for the exam, it is now time to focus on the eight domains.

1. **Security And Risk Management**

The biggest portion of the exam taking up 15% of the questions, this section covers confidentiality, integrity, availability, governance principles, compliance, legal issues, IT policies, and risk-based management concepts.

2. **Asset Security**

Boasting a range of questions that tackle the classification of assets, privacy, retention periods, data security controls, and handling requirements, this section is 10% of the exam.

3. **Security Architecture And Engineering**

Taking up 13% of the total exam, this section looks at secure design principles, security model fundamentals, security capabilities, vulnerability assessment, cryptography, implementation of physical security, and more.

4. **Communications And Network Security**

Focused on the network, this domain takes 14% of the questions to cover secure network architecture principles, components, and communication channels.

5. **Identify And Access Management**

Used to assure a candidate's ability to control user access to data, 13% of the exam is dedicated to this domain. These questions cover physical access to assets, logical access to assets, identification, authentication, third-party ID services, authorization mechanisms, and associated lifecycle.

6. **Security Assessment And Testing**

Twelve percent of the exam encompasses assessment and testing strategies for design and performance of security. It covers control testing, security process data collection, outputs, as well as internal and third-party audits.

7. **Security Operations**

The creation and action of security plans, this domain uses 13% of the questions to test understanding, requirements, and types of investigations, as well as monitoring activities, provision resources, operation concepts, application of techniques, incident management, recovery, business continuity, and more.

8. **Software Development Security**

Finally, taking up 10% of the questions, this domain deep-dives into software security lifecycle development, controls of the environment, the effectiveness of software security, and coding standards.

Embarking On The CISSP Journey

The choice to take on the CISSP certification comes with a lot of hard work as well as many open doors into an interesting and ever-growing industry. Becoming part of a global community of professionals that fortifies a safe and secure digital world, this certification is a rewarding experience that countless people admire. Advancing into the elite of the Information Systems Security Professionals starts with this certification.