The Official CISSP Certification Boot Camp

5 Days Classroom Session | 5 Days Live Online

Overview

The CISSP certification has become the de facto standard of information security credentials. Long sought after in America and growing in Europe, the CISSP is a sweeping security management credential that establishes your literacy and credibility as an information security professional. With hacks and attacks on the rise everywhere you look, never has the investment in security certification been more worth it for the enterprise. With CISSP credential holders earning salary averages of $114k or more, the credential is well worth it to the individual practitioner as well.

Led by real-world experts in information security who are authorized (ISC)² instructors, the Official (ISC)² CISSP Certification Boot Camp is the most comprehensive review of information security concepts and industry best practices. This course covers the ten domains of the CISSP CBK (Common Body of Knowledge). This training course reviews and refreshes your information security knowledge and helps identify the areas you need to study for the CISSP exam.

- Identify the purpose, benefits, and process of information classification and how it is used for Access Control policies and identifying the process for assessing the effectiveness of implemented controls.
- Master basic understanding of telecommunication and network security concepts.
- Learn the required components for minimizing security risks, securing channels of communication, and techniques for preventing and detecting network-based attacks.
- Apply the Information Security Governance and Risk Management framework including the policies, concepts, principles, structures and standards that are established for the protection of information assets, and how to assess the effectiveness of that prote
- Navigate the details of Software Development Security, including the activities and processes pertaining to the planning, programming, and management of software and systems that manage software including ways to secure applications through design and con
- Work with Cryptography concepts, including application of public and private algorithms, distribution management, methods of attack, and the application, development, and use of digital signatures for authenticity and electronic transactions, and nonrepud
- Use the Security Architecture and Design concepts focusing on the architecture of security systems that provide for the availability, integrity, and confidentiality of organizational assets.
- Master key terms and processes of Security Operations and how to protect and control information processing assets in a centralized or distributed environment – use daily tasks required to keep security services operating reliably and efficiently.
- Identify and apply the Business Continuity and Disaster Recovery Planning requirements necessary to develop the preparation, processes, and practices necessary to ensure the preservation of the business in case of major disruptions to normal business oper
- Evaluate the physical, environmental, and procedural risks that might be present in a facility,
- organization, or structure where information systems are stored and managed.