TEKNOLOGISK INSTITUT

Kursus
5 dage
Nr. 90519 A

DKK 22.499
ekskl. moms

Dato
07-10-2024

Sted
Taastrup

CISSP Bootcamp

På dette forberedelseskursus til den internationale certificering Certified Information System Security Professional - CISSP får du en dybdegående og intensiv gennemgang af de 8 domains samt tips og gode råd til, hvordan du forbereder dig til 2024 (ISC)² eksamen. Selve CISSP certificeringen anses for at være den førende inden for informationssikkerhed. Undervisningen foregår på engelsk og eksamen er ikke inkluderet i kurset.

Certified Information System Security Professional

Now completely updated for the 2024 exam refresh. (ISC)² Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the not-for-profit International Information Systems Security Certification.
The certification itself is seen as the world's premier certification for information security professionals. The CISSP Bootcamp includes in-depth & intense coverage of all eight domains plus tips and advice to prepare yourself for the new 2024 (ISC)²exam. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

Audience

The Bootcamp is designed for experienced security Professionals who wish to attain (ISC)² CISSP certification and should not be taken lightly. Students must have at least 2-5 years experience in the field of security.

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

Prerequisites

To attend this training, students must have at least 2-5 years of experience in the field of security (basic concepts, standards and framework within IT Security). A background from technical IT security in networking, web security, cryptografi, authentication or background architecture / design of systems within IT is useful. The course spans wide across many different areas, and knowledge from one or more areas within security is a definite advantage.

Pre-requisites for the exam

You need to document a minimum of 5 years experience within at least 2 of the 8 knowledge areas in the CISSP curriculum, to be CISSP certified.

Det får du på arrangementet

- Erfaren underviser
- Fuld forplejning
- Gratis parkering
- Materiale på engelsk
- Undervisning på engelsk

Course overview

The CISSP draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices. The CISSP exam tests one's competence in the 8 domains of the CISSP CBK, which cover:

- Introductions and Pre-course Test
- Domain 1: Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity)
- Domain 2: Asset Security (Protecting Security of Assets)
- Domain 3: Security Engineering (Engineering and Management of Security)
- Domain 4: Communications and Network Security (Designing and Protecting Network Security)
- Domain 5: Identity and Access Management (Controlling Access and Managing Identity)
- Domain 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Domain 7: Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
- Domain 8: Software Development Security (Understanding, Applying, and Enforcing Software Security)
- Post Course Test
- CISSP Exam Preparation & Review Questions

Learning Objective

- Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness and Implement risk management and the principles used to support it (Risk avoidance, Risk acceptance, Risk mitigation, Risk transference).
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and address the frameworks and policies, concepts, principles, structures, and standards used to establish criteria for the protection

of information assets, as well as to assess the effectiveness of that protection and establish the foundation of a comprehensive and proactive security program to ensure the protection of an organization's information assets.
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and examine the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authenticity.
- Understand the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media and identify risks that can be quantitatively and qualitatively measured to support the building of business cases to drive proactive security in the enterprise.
- Offer greater visibility into determining who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture.
- Plan for technology development, including risk, and evaluate the system design against mission requirements, and identify where competitive prototyping and other evaluation techniques fit in the process.
- Protect and control information processing assets in centralized and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently. Understand the Software Development Life Cycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security.

Courseware

All students receive a copy of:

- The Official (ISC)² Guide to the CISSP CBK
- CISSP Exam Self-Practice Review Questions.
- Also provided are practice test and tip sheets. All designed to fine tune your skills in preparation to take the exam.

Certification

This course, along with previous experience and rigorous self-study will help prepare you to take the following (ISC)² certification exam CISSP.

Exam and exam fee are not included in this course. You can read more about the exam at (ISC)² and register for the exam here.

Candidates for the CISSP must meet several requirements:

- Candidates must have a minimum of 5 years cumulative paid work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience. A candidate that doesn't have the required experience to become a CISSP may become an Associate of (ISC)² by successfully passing the CISSP examination. The Associate of (ISC)² will then have 6 years to earn the 5 years required experience.
- Pass the CISSP exam with a scaled score of 700 points or greater out of 1000 possible points. The exam is multiple choice and advanced innovative questions, consisting of 100-150 questions, to be answered over a period of three hours.

Aktuelt onlinekursus

Onlinekurset "Certified Information Systems Security Professional (CISSP) 2021" kunne også være interessant for dig.

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

UNDERVISER

Andy Malone

Andy kommer fra Skotland og har mere end 23 års erfaring med undervisning og konsulentarbejde. Han er en meget anerkendt Microsoft Certified Trainer (MCT), men er også for 14. år i træk kåret som Microsoft MVP (Most Valuable Professional). Andy er specialiseret i Microsoft Cloud, Identity, Authentication og Information Security, og han leverer undervisning af høj kvalitet med et glimt i øjet.

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk