UNSW CANBERRA | Cyber

CISSP Training

Location	UNSW Canberra
Duration	5 days
Standard Price	$3,706.00
Defence Price	$3,370.00

Description

Led by an (ISC)² authorised instructor, this training course provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features:

- Official (ISC)² courseware
- Taught by an authorised (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Learning Outcomes

On completion of this course, participants should be able to:

- Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness.
- 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.
- Offer greater visibility into determining who or what may have altered data or system information.
- Plan for technology development, including risk, and evaluate the system design against mission requirements.
- Protect and control information processing assets in centralised and distributed environments.

Who Should Attend

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect

NICE Framework mapping

This course maps to the highlighted work categories:

Securely Provision | **Oversee & Govern** | **Analyse** | **Investigate**

Operate & Maintain | **Protect & Defend** | **Collect & Operate**

To find out more about the NICE Framework go to: niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Further Information

Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on eight adult learning theories:

1. 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.
2. 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).
3. Apply a comprehensive and rigorous method for describing a current and/or future structure and behaviour for an organisation's security processes, information security systems, personnel, and organisational sub-units so that these practices and processes align with the organisation'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 organisation's information assets.
4. Apply a comprehensive and rigorous method for describing a current and/or future structure and behaviour for an organisation's security processes, information security systems, personnel, and organisational sub-units so that these practices and processes align with the organisation'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.
5. 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.
6. 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 organisations to have a better understanding of the state of their security posture.
7. Protect and control information processing assets in centralised and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently.
8. 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.

UNSW Canberra Cyber

UNSW Canberra Cyber is a unique, cutting-edge, interdisciplinary research and teaching centre, working to develop the next generation of cyber security experts and leaders. The centre is based in Canberra at the Australian Defence Force Academy and provides professional, undergraduate and post graduate education in cyber security. Our air-gapped, state of the art cyber range offers a secure environment where we deliver a number of technical and highly specialised learning opportunities. Our courses are designed to give the next generation of cyber security professionals the skill sets needed to thrive in the industry. We can also create bespoke professional education programs tailored to your organisation's needs. Contact us at cyber@adfa.edu.au to discuss how.

Find out more

cyber@adfa.edu.au
unsw.adfa.edu.au/cyber