CTR-909 CSMP - Cyber Security Methodology Professional

About this course

This is a 40-hour course designed to train cyber defense experts who can advise, guide, and make decisions on information protection tasks focusing on the administrative-government aspects (without the technological-tactical aspects domain). These abilities will be acquired through a thorough familiarity with knowledge of international, national, sectoral, and business standards, and familiarity with organizational policy, procedures, and best practices in these areas, including management techniques. Students will gradually learn the core features of the CSMP through lectures, self-guided homework assignments, and in-vivo practice labs. This course closely follows the instructions of the National Cyber Protection Authority on the one hand, and on the other hand, the needs and standards of the Ministry of Defense and of other international organizations such as ISACA, (ISC)2, CSA, and ISO 27001.

Audience profile

This course is designed for individuals with a background in infrastructure, IT, or cybersecurity professionals, or those with a background in development, with an organizational background.

At course completion

After completing this course, students will be able to:

- Oversee the strategy and justifications for cyber security approaches; make choices on information security responsibilities with a focus on administrative-government issues (without the technological-tactical aspects domain).
- Understand developed process includes six sequential steps conducted by three teams (an operationally focused team, a cybersecurity-focused team, and a system engineering team).

Course details

Module 1: Introduction to Cyber Governance, Risk, and Compliance (GRC)

This module will teach about security standards, policies, and compliance. You will understand the policy documents, know how to comply with laws and regulations, and adopt standards and frameworks such as ISO 27001, PCI-DSS, HIPPA, GLBA, and more.

Module 2: Risk Management and Privacy

This module explains what it means to analyze risk, manage risk, and third-party management. You will learn about personnel management.

Module 3: Disaster Recovery Planning

This module addresses disaster recovery and business continuity. It talks about the laws and acts, implementations, and improvement tools.

Module 4: Infosec Governance Risk and Compliance
This lesson digs into strategic planning for governments, program management, auditor preparedness, and environmental control.

Module 5: CISO Function and Role
This module examines capital planning and investment control, InfoSec processes, and policies. You'll learn how to measure society as it pertains to CISO core functions and business continuity.

Prerequisites

- Entry Level exam (American test)
- Ideally- Previous background in IT and/or cybersecurity
- Organizational background
- Readability to invest in self-guided homework assignments