Overview

Cybersecurity Management I - Strategic focuses on the strategic and long-term alignment of an organization's information security program to regulators and ensures that it is appropriate for the company culture and management organization. This course introduces the Basel Committee's four lines of defense model to appropriately implement separation of duties and information security roles and structures. Additionally, this course covers big-picture items (e.g., how risk management will be performed institutionally and how compliance to information security requirements will be managed). Finally, this course helps students apply strategic decision making as companies adapt to new technologies, processes, and people practices related to processing, managing, and protecting information resources. The Cybersecurity Architecture and Engineering course is a prerequisite for this course.

Competencies

- **Readiness**
  This competency exists to assess the readiness of students.

- **Continual Improvement**
  The graduate evaluates organization-wide security controls to support continual improvement.

- **Identity and Access Management**
  The graduate manages the identity and access provisioning lifecycle to protect data and systems.

- **Laws, Regulations, and Compliance**
  The graduate manages compliance practices for cybersecurity and information assurance.

- **Development of Business Continuity**
  The graduate develops business continuity plans to maintain an organization's ability to perform its mission-critical tasks.

- **Risk Management**
  The graduate manages risk in the face of an ever-changing technology landscape.
The graduate designs an organizational structure to support an information security policy.

The graduate develops security policy, standards, procedures, and guidelines to strategically secure an organization's assets.

Learning

Getting Started

Welcome to Cybersecurity Management I - Strategic! In this uCertify course, you will encounter readings, educational media, and interactive knowledge checks. Complete each lesson and deepen your grasp of the main concepts using the tools provided. Competency will be demonstrated by the successful completion of an objective assessment and a performance assessment. The Topics and Pacing, included in the “Welcome” section of the course, provides a suggested weekly plan for working through the materials in a timely manner.

Assessments

Pre-Assessment: Cybersecurity Management I - Strategic (CJO2)

STATUS: Not Attempted

TIME ALLOTED: 150 minutes

# OF ITEMS: 70

CODE: PAQG

Objective Assessment: Cybersecurity Management I - Strategic

STATUS: Not Attempted
A score of Competent or Exemplary is required to pass all assessments. Passing a preassessment does not guarantee you will pass the high stakes assessment.

On objective assessments, you will be charged a retake fee for the third attempt and every attempt thereafter. For more information click here.
Course Instructor

Course Instructor Group

cmsecurity@wgu.edu

Schedule an Appointment with any Course Instructor

Course Instructor Responsibility

How to Work with Course Instructors

Announcements

Course Tips

Course Search

Course Chatter