Cybersecurity Management II - Tactical – C795

Overview

Cybersecurity Management II - Tactical provides students the opportunity to examine tactical cybersecurity management, which is the practice of addressing near-term cybersecurity goals within an enterprise. The tactical management process enables organizations to address unique cyber requirements throughout the organization. It deals with the people, processes, and technologies that are in use, and it primarily centers on the current operations of the enterprise. A range of cybersecurity tactical management topics are introduced in this course including the tools, techniques, and concepts used to develop an effective cybersecurity program within organizations. The Cybersecurity Management I - Strategic course is a prerequisite for this course.

Competencies

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

- **Business Continuity**
  The graduate executes disaster recovery and business continuity plans and procedures.

- **Critical Security Controls**
  The graduate develops defense-in-depth practices to mitigate cybersecurity threats to organizations.

- **Enterprise Security Policies**
  The graduate manages IT security policies to support an effective cybersecurity operation within an organization.

- **Security Assessment and Testing**
  The graduate manages security assessment and testing tactics.

- **Detective and Preventive Measures**
  The graduate manages detective and preventive security measures.

- **Cybersecurity Incident Response**
Getting Started

Welcome to Cybersecurity Management II - Tactical! In this uCertify course, you will encounter videos, labs, 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 II - Tactical (FMO2)
STATUS: Not Attempted
TIME ALLOCATED: 150 minutes
# OF ITEMS: 70
CODE: PFMO

Objective Assessment: Cybersecurity Management II - Tactical
STATUS: Not Attempted
TIME ALLOCATED: 150 minutes
# OF ITEMS: 70
Diagnostic: Cybersecurity Management II - Tactical

STATUS: Not Attempted

TIME ALLOCATED: 150 minutes

# OF ITEMS: 11

CODE: XFMO

Performance Assessment: Cybersecurity Management II - Tactical - BBM1

Task 1 Not Submitted

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 Responsibility

How to Work with Course Instructors

Announcements

Course Tips

Course Search

Course Chatter