CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF WEST FLORIDA

Risk Management

UWF Florida Cybersecurity Training Program

Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course / Cyber Skills Exercise Dates: Feb. 26-Mar. 8, 2024

Cyber Skills Exercise Times: N/A

Duration: 2 weeks.

Estimated Time Completion: 15-25 hours.

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online with weekly instructor Zoom sessions.

Target Audience: Anyone with technical or non-technical responsibilities for establishing, maintaining, managing, mitigating, and addressing IT/cyber risk management at all levels of the organization.

Requires Prerequisites / Background: None.

CEU's: 1.5, **CPE's:** 18

Course Instructor

Instructor	Email Address
Guy Garrett, M.S., M.B.A.	ggarrett@uwf.edu

Course Description

This course focuses on the fundamentals of risk management as applied to cybersecurity and privacy. Risk is addressed using the NIST Risk Management Framework in addition to the requirements of Florida Administrative Rules. This course includes scenario-based exercises and an introduction to system categorization.

Student Learning Outcomes:
Upon completion of the course, students will be able to:

- Participate in an information security risk assessment (T0158)
- Participate in the development or modification of the computer environment cybersecurity program plans and requirements (T0159)
- Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle (T0263)
- Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc…(T2064)
- Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals (T0265)
- Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
- Demonstrate knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K0002)
- Demonstrate knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. (K0038)
- Demonstrate the ability to understand the basic concepts and issues related to cyber and its organizational impact. (A0119)
- Demonstrate the ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (A0123)

NIST NICE Cybersecurity Workforce Framework Mapping

Work Roles

- Authorizing Official (SP-RSK-001)
- Information Security Systems Manager (OV-MGT-001)

Course Information

Materials: Provided through the Canvas LMS.

Recommended Resources

Guide for Conducting Risk Assessments, SP 800-30, Rev. 1.
https://csrc.nist.gov/publications/sp800

Florida Rule 60GG-2 Information Technology Standards
https://flrules.org/gateway/ChapterHome.asp?Chapter=60GG-2

Building an Information Technology Security Awareness & Training Program, SP 800-50
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Technical Specifications:

Students need high-speed Internet access, a current web browser (Chrome/Firefox tend to work best), Adobe Reader and MS Office or similar software.

By enrolling for this course, I agree to abide by the Computing Resource Usage Agreement provided to me.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	**Percentage**
Quizzes/Labs	50%
Scenario-based exercises/work packages	50%
Total:	**100%**

Student Accessibility Resources:

If you have a disability that impacts your full participation in this course, please email Student Accessibility Resources at 850.474.2387 or by email, sar@uwf.edu.

Course Outline

Module	**Activities / Assessments**
M01 – Risk Related Cyber Concepts	Quiz
M02 – Requirements & Roles	Quiz
M03 – RMF Prepare & Categorize	Scenario-based exercise part 1 Lab: Intro to System Categorization
M04 – RMF Select & Implement	Scenario-based exercise part 2

	Lab: Intro to Controls
M05 – RMF Assess, Authorize, Monitor	Scenario-based exercise part 3 Quiz