



Course Outcome Summary

Required Program Core Course

CIA 202 Risk Vulnerability Analysis

Course Information

Division	Business
Contact Hours	45
Total Credits	3

Prerequisites

CIA 103 Information Security Principles (formerly IAS 103)

Course Description

This course covers tools, techniques, and methodologies for physical risk analyses. Students will study Security Best Practices and audit requirements for specific environments. Topics to be covered include internal and external penetration tests, wireless security technology, risk analysis methodology, and security audits. This course aims to provide undergraduate level students with an educational experience in the application of risk management theory and principles to information security policy, information systems computer and network facilities, and the life cycle development process.

This course is a required core course for students pursuing an:
AAS in Cybersecurity and Information Assurance

Course Outcomes

To evidence success in this course, the students will be able to:

- CIA 202 CSLO 01 - Define Information Assurance;
- CIA 202 CSLO 02 - Define and Demonstrate Risk Management and Risk Analysis;
- CIA 202 CSLO 03 - Demonstrate vulnerability assessment techniques;
- CIA 202 CSLO 04 - Demonstrate threat analysis techniques;
- CIA 202 CSLO 05 - Apply threat matrix analysis;
- CIA 202 CSLO 06 - Plan vulnerability assessment, threat assessment, and risk analysis projects;
- CIA 202 CSLO 07 - Apply risk management principles throughout the software and systems development life cycles to include continuity;
- CIA 202 CSLO 08 - Demonstrate Incident Handling, Continuity, and Disaster Recovery techniques;
- CIA 202 CSLO 09 - Define Network Security assessment and Accreditation techniques;

Program Outcomes Addressed by this Course:

Upon successful completion of this course, students should be able to meet the program outcomes listed below:



Cybersecurity and Information Assurance

CIA 202 CSLO 01 - Define Information Assurance;

Applies to Cybersecurity and Information Assurance Program level Student Learning Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 02 - Define and Demonstrate Risk Management and Risk Analysis;

Applies to Cybersecurity and Information Assurance Program level Student Learning Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 03 - Demonstrate vulnerability assessment techniques;

Applies to Cybersecurity and Information Assurance Program level Student Learning Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 04 - Demonstrate threat analysis techniques;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 05 - Apply threat matrix analysis;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 06 - Plan vulnerability assessment, threat assessment, and risk analysis projects;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.



MONROE COUNTY
COMMUNITY COLLEGE

Course Outcome Summary

Required Program Core Course

CIA 202 Risk Vulnerability Analysis

CIA 202 CSLO 07 - Apply risk management principles throughout the software and systems development life cycles to include continuity;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 08 - Demonstrate Incident Handling, Continuity, and Disaster Recovery techniques;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

CIA 202 CSLO 09 - Define Network Security assessment and Accreditation techniques;

Applies to Program Outcome

CY PSLO 06 - Identify and explain risk and potential security issues.

CY PSLO 08 - Demonstrate foundation knowledge of information security/assurance within the organization.

Date Updated:4/13/2022

By: William Hilliker