MONROE COUNTY COMMUNITY COLLEGE
enriching lives

Risk Vulnerability Analysis
Outline of Instruction

Course Information

Organization	Monroe County Community College
Developers	William Hilliker
Course Number	IAS 202
Division	Business

Description
This course covers tools, techniques, and methodologies in performing computer system and network security vulnerability risk analyses. Security Best Practices and audit requirements for specific environments will be studied. Topics to be covered include internal and external penetration tests, wireless security technology, risk analysis methodology, and security audits. The purpose of this course is 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.

Major Units
Unit 1: Risk Management Fundamentals Exploits
Unit 2: Managing Risk: Threats, Vulnerabilities, and
Unit 3: Maintaining Compliance
Unit 4: Developing a Risk Management Plan
Unit 5: Defining Risk Assessment Approaches
Unit 6: Performing a Risk Assessment
Unit 7: Identifying Assets and Activities to be Protected
Unit 8 Identifying and Analyzing Threats, Vulnerabilities and Exploits
Unit 9: Identifying and Analyzing Risk Mitigation Security Controls
Unit 10: Planning Risk Mitigation Throughout Your Organization
Unit 11: Turning Your Risk Assessment into a Risk Mitigation Plan
Unit 12: Mitigating Risk with a Business Impact Analysis
Unit 13: Mitigating Risk with a Business Continuity Plan
Unit 14: Mitigating Risk with a Disaster Recovery Plan
Unit 15: Mitigating Risk with a Computer Incident Response Team Plan

Prerequisites
CIS 130 and IAS 103

Exit Learning Outcomes
Program Outcomes
A. Demonstrate knowledge of the profession, its organizations, goals and leadership roles, literature/publications, issues, and research foundations.
B. Demonstrate foundation knowledge of information security/assurance within the organization.
C. Demonstrate knowledge of security objectives and policy development.
D. Demonstrate an understanding of risk management, risk assessment, vulnerability assessment, and take preventative measures against the threats.
E. Demonstrate business continuity and disaster recovery techniques.

Course Outcomes

In order to evidence success in this course, students will be able to:

1. Define information assurance

Linked Program Outcomes

Demonstrate knowledge of the profession, its organizations, goals and leadership roles, literature/publications, issues, and research foundations.

Demonstrate foundation knowledge of information security/assurance within the organization.

Demonstrate knowledge of security objectives and policy development.

2. Define and Demonstrate risk management and risk analysis

Linked Program Outcomes

Demonstrate an understanding of risk management, risk assessment, vulnerability assessment, and take preventative measures against the threats.

Demonstrate business continuity and disaster recovery techniques.

3. Demonstrate vulnerability assessment techniques

Linked Program Outcomes

Demonstrate an understanding of risk management, risk assessment, vulnerability assessment, and take preventative measures against the threats.

Demonstrate business continuity and disaster recovery techniques.

4. Demonstrate threat analysis techniques

Linked Program Outcomes

Demonstrate knowledge of security objectives and policy development.

5. Apply threat matrix analysis

Linked Program Outcomes

Demonstrate knowledge of security objectives and policy development.

Demonstrate an understanding of risk management, risk assessment, vulnerability assessment, and take preventative measures against the threats.

6. Plan vulnerability assessment, threat assessment and risk analysis projects

Linked Program Outcomes

Demonstrate knowledge of security objectives and policy development.

Demonstrate an understanding of risk management, risk assessment, vulnerability assessment, and take preventative measures against the threats.

Demonstrate business continuity and disaster recovery techniques.

7. Apply risk management principles throughout the software and systems development life cycles to include continuity.

Linked Program Outcomes

Demonstrate foundation knowledge of information security/assurance within the organization.

Demonstrate knowledge of security objectives and policy development.

8. Demonstrate Incident Handling, Continuity, and Disaster Recovery techniques

Linked Program Outcomes

Demonstrate business continuity and disaster recovery techniques.

9. Define Network Security assessment and Accreditation techniques

Linked Program Outcomes

Demonstrate knowledge of the profession, its organizations, goals and leadership roles, literature/publications, issues, and research foundations.