

**WILIMINGTON UNIVERSITY  
COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES  
BASIC COURSE INFORMATION**

**COURSE TITLE:** Risk Analysis and Management

**COURSE NUMBER:**

**II. RATIONALE:**

In the post 9-11 era, risk analysis concepts and methodologies are evolving rapidly. Although models differ in the definition, labeling and sequencing of steps, there is solid consensus on the essential components. It is not possible to completely eliminate risk. Therefore it is important to determine what level of protection is desirable, and which countermeasures, strategies and options can help to achieve this level. Students should be exposed to the toolkit of current analysis and assessment methodologies used by practitioners today to define, quantify, calculate and respond to security risk. These processes are known as risk management and physical security program design.

**III. MAJOR INSTRUCTIONAL GOALS:**

**GOAL A:** The student will demonstrate an understanding of the key components of risk analysis.

**Learning Outcome:** The student will:

- A-1 Define critical infrastructure and key asset inventory
- A-2 Define criticality assessment
- A-3 Define threat assessment
- A-4 Define vulnerability assessment

**GOAL B:** The student will demonstrate an understanding of the relationships between key components used to analyze risk.

**Learning Outcome:** The student will:

- B-1 Describe quantitative risk assessment and the annual loss expectancy (ALE) equation
- B-2 Describe qualitative risk assessment
- B-3 Identify the risk analysis equation
- B-4 Prepare a matrix based risk analysis grid
- B-5 Prepare a risk analysis flow chart

**GOAL C:** The student will demonstrate an understanding of the different types of risk assessment methodologies in use by security practitioners today.

**Learning Outcome:** The student will:

- C-1 Discuss the CARVER method and the CARVER + Shock
- C-2 Discuss the ASIS seven step approach to risk assessment
- C-3 Discuss the ARM methodology
- C-4 Discuss the DOJ/IACP methodology

**GOAL D:** The student will demonstrate an understanding of physical security program design and development.

**Learning Outcome:** The student will:

- D-1 Describe the elements of a security plan
- D-2 Describe the phases in the development of a physical security plan
- D-3 Explain the differences between a security survey and a security audit
- D-4 Identify the key components of a physical security survey

**GOAL E:** The student will demonstrate an understanding of physical security program protection measures and the development of a protection strategy.

**Learning Outcome:** The student will:

- E-1 Describe physical security protection categories and the interrelationship between physical security countermeasures
- E-2 List the types of physical security countermeasures that can be used to reduce risk
- E-3 Assign relative costs to security countermeasures and perform benefits comparisons

**GOAL F:** Apply theory to practical in a manner that demonstrates a comprehension of the elements of risk analysis and the conduct of physical security assessments.

**Learning Outcome:** The student will:

- F-1 Perform a risk analysis and conduct a physical security survey for a selected business entity that reflects the application of course goals and objectives
- F-2 Develop a written physical security protection strategy for the selected business entity that confirms comprehension of course materials