BELLEVUE UNIVERSITY

Course Syllabus Part I
CIS 411 Assessments and Audits

3 Credit Hours

Course Description

This course is intended to introduce students to the principles of risk assessment, vulnerability analysis, and auditing and how they are used to evaluate the effectiveness of information security controls. Students will develop an understanding of threat and asset identification, countermeasures, and safeguards, acceptable risks, and vulnerabilities. The auditing concepts of technical, physical, and administrative controls will also be introduced along with how these controls are measured for effectiveness.

Course Prerequisites

None

Course Objectives

Students who successfully complete this course should be able to:

1. Demonstrate vulnerability identification and assessment tools and processes based on real scenarios.
2. Appraise threats to an organization and its IT assets.
3. Identify threats, vulnerabilities, risks, and effective countermeasures for a sample organization.
4. Organize an IT Audit for a sample organization, to include analysis of technical, physical, and administrative controls.
5. Evaluate the effectiveness of security controls originating from international standards.
6. Construct an assessment for a sample organization to determine critical vulnerabilities.

Grading Scale

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

Topic Outline

I. Overview of Assessments and Audits
   a. Risk management
   b. Compliance
   c. Asset identification
   d. Vulnerability management

  e. Threat landscapes
  f. Auditing IT controls

II. Vulnerability Assessments
  a. Vulnerability management process lifecycle
  b. Identification
  c. Analysis
  d. Mitigation

III. Threat Assessments
  a. Threat landscape
  b. Identification
  c. Analysis

IV. IT Audit Process
  a. IT Audit plan development
  b. Measuring effectiveness of IT Controls
  c. Evidence collection
  d. Reporting

V. Overview of Frameworks, Standards, & Regulations
  a. ISO 27001
  b. COSO
  c. CobiT
  d. ISACA

VI. Establishing controls to reduce risks
  a. Policies
  b. Patch management process & tools
  c. Business continuity
  d. Awareness
  e. Technical controls
  f. Physical controls
  g. Administrative controls

VII. Case Studies
  a. Vulnerability assessment
  b. Threat assessment
  c. IT audit