

## COURSE SYLLABUS

Course Name: IA 546:  
Information Security Vulnerability & Risk Analysis  
Instructor: Gerald V. "Skip" Lawver  
Office Hours: Call for Appointment  
Office: Telephone: 734-487-3170  
Internet/E-Mail Address: [Skip.Lawver@emich.edu](mailto:Skip.Lawver@emich.edu)

### **Course Description:**

The identification of vulnerabilities and risks inherent in the operation and administration of information systems will be explored. Countermeasures will be discussed and documented in an effort to counter identified vulnerabilities.

### **Course Objectives:**

This course will assist students in their career preparation as information system security managers. Upon successful completion of this course, students should be able to:

1. Demonstrate risk management and risk analysis
2. Demonstrate vulnerability assessment techniques
3. Demonstrate threat analysis techniques
4. Plan vulnerability assessment, threat assessment and risk analysis projects
5. Prepare and present business based recommendations for expenditure of security funds
6. Apply risk management principles throughout the software and systems development life cycles to include continuity.

### **Purpose:**

The purpose of this course is to provide graduate 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.

**Scope:** The scope of the material to be covered includes:

- Risk analysis methodology, the fundamental theory of risk.
- Development of information security policy and programs based on a risk analysis approach;
- Application of risk analysis methodologies as they apply to the information systems field, and;
- The relationship of the risk management process to business objectives and/or organization mission and the maintenance of information systems.

### **Student Requirements:**

The overall goal of this course is to provide a practical educational experience in the fundamentals and application of risk management to the information security field. The highest level of student gain will be achieved by participation in the team-based directed exercise(s) and by participation in classroom activities as well as individual assignments.

Each student will be required to actively participate in the class exercises and contribute to the overall team effort. Students will be given reading assignments as well as assigned written projects.

**Required Texts and Handouts:** Students will receive reading assignments that may include handout material, and/or research searches, and is responsible to read and act on the material as directed. The required texts are:

**Primary Text:** Computer Security Handbook, fourth edition ed. Bosworth, Seymour, Kabay, M. E. pub. Wiley, Parts 2 and 5 (Required text for the entire MLS/IS program)

**Supplementary Text:** Enterprise Security – the Manager’s Defense Guide Clark, David Leon pub Addison Wesley, Part 4 (Required supplementary text for the entire MLS/IS program)

Various handouts as determined by your instructor

**Assessment and Evaluation:** The final grade for the class will be based on the following requirements as directed by your instructor: Team based development, presentation and evaluation of a final project, including a complete bibliography and areas of further research, as well as a Team Leaders evaluation of each group member individually, will account for 50% of each student’s grade.

Student participation in class activities will account for 50% of each student’s grade. This includes attendance which is required.

All points are cumulated, converted to percent form, and converted to letter grades based on this straight scale: 94% and above, A; 90% and above A-; 87% and above, B+; 84% and above, B; 80% and above, B-; 77% and above, C+; 74% and above, C; 70% and above, C-; 67% and above, D+; 64% and above, D; 60% and above, D-; below 60%, E.

#### **Notes on Requirements and Grading:**

Class sessions will involve interactive approach and student activities. Students are expected to have textbooks and other assigned materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, or other misc. materials including disks, or backup files (in case a file is lost or damaged).

Attendance at all times is required of all students, and failure to attend is considered lack of participation. Verifiable emergencies will only be considered.

#### **General Policies:**

Attendance and punctuality is mandatory. Class will start at the given time.

All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an un-interrupted class.

- Speak to the instructor as needed.
- Students should comply with expectations for use of the college and university laboratories and classrooms, with standards for fair information practices, and with licensing provisions of the software in use.
- Students must complete their own work when given an individual assignment. During team-based assignments they will work with one another to solve problems and develop the team-based project. Students who submit the work of other students,

including companies and organizations, as their own (Plagiarism), will be penalized to the full extent permitted by University policy.

- Late work is not accepted. Oral presentations may not be made up.
- Inability to prepare for an assignment and poor time management are not considered valid reasons for late work or re-scheduling. In addition, students must back up work, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions may involve some lecture, Caucus/Online, with mostly group-facilitated activities. Therefore, it is the student's responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
- Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
- Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.
- All assignments will be graded for compliance to the author's directions.
- Final grades will not be given in person, by telephone, e-mail, fax or any other communications median except that of University standard written grading at the end of the semester.
- Attendance/participation is required therefore it is the student's responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
- A grade of "I" will be given only in accordance with Eastern Michigan University's Graduate school guideline.
- By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

Course Content and Schedule: This schedule is an approximate timeline for the student.

## Unit 1: INTRODUCTION AND RISK MANAGEMENT

### Chapter 1 - 4

#### 1.1 Introduction and Risk Management

##### 1.1.1 Introductions

##### 1.1.2 Course Review and Intro

##### 1.1.3 Overview of the risk management process

##### 1.1.4 Cost/Benefit Analysis of Information Assurance

##### 1.1.5 Documentation

##### 1.1.6 Risk

##### 1.1.7 Risk Assessment

##### 1.1.8 Risk Management

##### 1.1.9 Residual Risk

##### 1.1.10 Risk Acceptance Process

##### 1.1.11 Systems Security Authorization Agreements (SSAA)

## Unit 2: THREATS

### Chapter 5

#### 2.1 Threats

##### 2.1.1 Vulnerability management

- 2.1.2 Introduction to vulnerability analysis
- 2.1.3 Attacks
- 2.1.4 Environmental/Natural Threats
- 2.1.5 Human Threats
- 2.1.6 Theft
- 2.1.7 Threat
- 2.1.8 Threat Analysis
- 2.1.9 Threat Assessment

### Unit 3: VULNERABILITIES

#### Chapter 5 & 8

- 3.1 Vulnerabilities
  - 3.1.1 Building a secure organization
  - 3.1.2 Evaluating strong authentication methods
  - 3.1.3 Vulnerabilities
  - 3.1.4 Vulnerability Analysis
  - 3.1.5 Network Vulnerabilities
  - 3.1.6 Technical Vulnerabilities

### Unit 4: ATTACKS AND COUNTERMEASURES

#### Chapter 8

- 4.1 Attacks and Countermeasures
  - 4.1.1 Information warfare
  - 4.1.2 Penetrating computing systems
  - 4.1.3 Malicious code
  - 4.1.4 Types of attacks
  - 4.1.5 Education, Training, and Awareness as Countermeasures
  - 4.1.6 Procedural Countermeasures
  - 4.1.7 Technical Countermeasures

### Unit 5: INCIDENT HANDLING AND RESPONSE

#### Chapter 15

- 5.1 Incident Handling and Response
  - 5.1.1 Vulnerability assessment tools
  - 5.1.2 Planning vulnerability and penetration tests
  - 5.1.3 Monitoring vulnerability and penetration tests
  - 5.1.4 Emergency Destruction Procedures
  - 5.1.5 Organizational/Agency Information Assurance Emergency Response Teams

### Unit 6: DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

#### Chapter 12

- 6.1 Disaster Recovery and Continuity of Operations
  - 6.1.1 Business Recovery - Importance
  - 6.1.2 Contingency/Continuity of Operations Planning
    - 6.1.2.1 Establishment and testing of contingency/continuity of operations plans
  - 6.1.3 Disaster Recovery
  - 6.1.4 Disaster Recovery Plan
    - 6.1.4.1 Establish and test disaster recovery plan
  - 6.1.5 Incident response policies
  - 6.1.6 Law enforcement interfaces/policies
  - 6.1.7 Reconstitution – principles and importance of
  - 6.1.8 Restoration

### Unit 7: CRITICALITY AND SENSITIVITY OF INFORMATION AND SYSTEMS

#### Chapter 4

## 7.1 Criticality and Sensitivity of Information Systems

### 7.1.1 Aggregation

### 7.1.2 Disclosure of Classified/Sensitive Information

## Unit 8: DEFINING NETWORK SECURITY AND ACCREDITATION OF SYSTEMS

Chapter 8 and 11 and handout material

### 8.1 Defining Network Security and Accreditation of Systems

#### 8.1.1 Memoranda of Understanding/Agreement (MOU/MOA)

##### 8.1.1.2 Facilitate development and execution of MOU/MOA

#### 8.1.2 Connectivity (interconnected organizations )

#### 8.1.3 Emissions Security (EMSEC) and TEMPEST

#### 8.1.4 Wireless Technology (electronic emanations, threats from electronic emanations )

Overview of the Semester Project:

Grading: There are 40 points for the semester project and presentation.

There are 60 points for participation in class activities, assignments and exams.

More on Planning the Project:

The class will be divided into groups to conduct a Risk Vulnerability Assessment of a fixed facility.

Cover page with all Team Members Names, etc.

Table of contents

Names of Team members and their individual responsibilities

The Team Leader is responsible for submitting each team member's participation and contributions to the project, which is to be included in the final document package.

Statement of the problem. What are the issues you are dealing with and why.

Summary statement focusing on the organization.

Solution Statement: How will you deal with the problems, issues, etc.

Bibliography

Areas of further research, including a preliminary research proposal on a significant information security problem related to Risk Analysis and/or Risk Management.

The focus of the final project will be determined at the start of each term.

A complete project with two hard (paper) copies being submitted as a total business document. Including a copy of the PowerPoint presentation. All documents must be secured in a Lightweight (paper) binder.

### **Academic Dishonesty**

In any university-level course, a statement of policy recognizing academic dishonesty should be unnecessary. However, it should be noted that the policy of the Department of Business and Technology Education is that, any student found to have engaged in any activity constituting academic dishonesty, will receive an "E" for the course in which the activity occurred. This policy relates to all forms of work associated with the course requirements; including examinations, quizzes, laboratory work, and all other assignments. It is the student's responsibility to review the page(s) of the graduate catalog in order to determine those activities, which constitute academic dishonesty at Eastern Michigan University, which include both cheating and plagiarism. This policy will be strictly enforced.

Definition Reminders:

Assist "To help or support." The American Heritage College Dictionary, 3rd Edition, page 83. Cheat "To act dishonestly, practice fraud. To violate rules deliberately." The American Heritage College Dictionary, 3rd Edition, page 239.

DUE: Accepted only during the class session during which you present your project. Print all components of the finished project, tables, queries, forms and reports. These should be assembled in logical order. Grading also includes: Correctness and accuracy of work, contents, professionalism, APA formatting, and other factors emphasized in the course or in the final project description. The team leaders evaluation is also to be submitted at this time, as well as a copy of the powerpoint presentation.

\*\*\*The Instructor reserves the right to make any additions/deletions or changes to this syllabus as deemed necessary.