Syllabus for CYB-5700

CYBER RISK MANAGEMENT AND INCIDENT RESPONSE

COURSE DESCRIPTION

This course delves into practical methods and techniques used for assessing and managing cybersecurity risks to an organization. Both quantitative and qualitative risk assessment methodologies are covered. Common cybersecurity risk assessment/management models and frameworks are evaluated and applied. Another major area of focus is cyber incident response and contingency planning consisting of incident response planning, disaster recovery planning, and business continuity planning.

COURSE TOPICS

- Cyber risk management frameworks and standards
- Assessing cybersecurity risks, vulnerabilities, and threats
- Qualitative and quantitative approaches to cyber risk management
- Informed cyber risk management business cases
- Risk reporting and monitoring
- Cyber incident response
- Contingency planning

COURSE OBJECTIVES

After completing this course, students should be able to:

CO 1 Articulate the need for cybersecurity (cyber) risk management methodologies and frameworks to defend information systems data and assets.

CO 2 Apply common industry terms through analysis of fundamental cyber risk management concepts.

CO 3 Outline elements of cyber risk management and the types of cybersecurity capabilities and controls applied to mitigate cyber risk based on accepted cyber risk management frameworks and standards.

CO 4 Categorize cyber risk with respect to mission goals, technology, and individuals in the enterprise and recommend effective responses.

CO 5 Assess the linkage among assessment components involving risk mitigation, security capabilities, and controls applied to functional areas of a system.

CO 6 Measure the impact of potential cyber threat events and vulnerabilities.

CO 7 Develop a cybersecurity risk mitigation strategy with applicable mitigation controls for an information system.

CO 8 Prepare scenario-based presentations to potential decision makers with supporting data of cyber risk and mitigation strategies.

CO 9 Apply cyber risk management methodologies and frameworks to provide effective and robust cyber incident response.

CO10 Evaluate a contingency plan and a course of action that allows an organization to respond effectively to a cyber event.

COURSE MATERIALS

You will need the following materials to complete your coursework. Some course materials may be free, open source, or available from other providers. You can access free or open-source materials by clicking the links provided below or in the module details documents. To purchase course materials, please visit the University's textbook supplier.

Required Textbook

- Hodson, C. J. (2019). *Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls*. New York, NY: Kogan Page Limited.
  ISBN-13: 978-0749484125

COURSE STRUCTURE

Cyber Risk Management and Incident Response is a three-credit, online course consisting of **six** modules. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

- **Module 1: Cyber Risk and Enterprise Risk Management Process**
  Course objectives covered in this module: CO 1, CO 2

- **Module 2: Cyber Risk Management Process for Organizations**
  Course objectives covered in this module: CO 3, CO 4

- **Module 3: Cyber Risk Management Process for Information Systems**
  Course objectives covered in this module: CO 4, CO 5

- **Module 4: Cyber Risk Assessment Process**
  Course objectives covered in this module: CO 5, CO 6, CO 7

- **Module 5: Cyber Incident Response**
  Course objectives covered in this module: CO 8, CO 9

- **Module 6: Contingency Planning**
  Course objectives covered in this module: CO 9, CO 10

ASSESSMENT METHODS

For your formal work in the course, you are required to participate in online discussion forums, complete written assignments, and complete a final project. See below for details.

Consult the Course Calendar for due dates.

Promoting Originality

One or more of your course activities may utilize a tool designed to promote original work and evaluate your submissions for plagiarism. More information about this tool is available in SafeAssign.

Discussion Forums

In addition to an ungraded About Me Forum, you are required to participate in **six** graded online class discussions.

Communication with your mentor and among fellow students is a critical component of online learning. Participation in online class discussions involves two distinct activities: an initial response to a discussion question and at least two subsequent comments on classmates' responses.

All of these responses must be substantial. Meaningful participation is relevant to the content, adds value, and advances the discussion. Comments such as "I agree" and "ditto" are not considered value-adding participation. Therefore, when you agree or disagree with a classmate or your mentor, state and support your position.

You will be evaluated on the quality and quantity of your participation, including your use of relevant course information to support your point of view, and your awareness of and responses to the postings of your classmates. Remember, these are discussions: responses and comments should be properly proofread and edited, mature, and respectful.

Written Assignments

You are required to complete **seven** written assignments. The written assignments are on a variety of

topics associated with the course modules. For specific details, consult the individual course modules.

Consult the Course Calendar for due dates.

📋 *Final Project*

You are required to complete **one** final project. For this final project, you will perform a cyber risk assessment using an assessment tool for a specific organization. The main purpose of this project is to determine and illustrate the importance of measuring gaps between current risk posture and target risk posture.

Reference the Final Project area of the course website for full requirements and instructions. Consult the Course Calendar for due dates.

📋 *Course Reflection*

For this course—and throughout the Master of Science in Cybersecurity (MSCYB) program—you will complete a course reflection, which includes collecting digital artifacts, participating in course reflection discussion forums, and writing a course reflection essay.

Reference the Course Reflection section of the course website for full requirements and instructions. Consult the Course Calendar for due dates.

GRADING AND EVALUATION

Your grade in the course will be determined as follows:

- **Online discussions (6)**—20%
- **Written assignments (7)**—45%
- **Final project**—20%
- **Course reflection**—15%
    - **Course reflection discussions (2)**—5%
    - **Course reflection essay**—10%

All activities will receive a numerical grade of 0–100. You will receive a score of 0 for any work not submitted. Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	=	93–100	B	=	83–87
A–	=	90–92	C	=	73–82
B+	=	88–89	F	=	Below 73

To receive credit for the course, you must earn a letter grade of C or higher on the weighted average of all assigned course work (e.g., assignments, discussion postings, projects.). Graduate students must maintain a B average overall to remain in good academic standing.

STRATEGIES FOR SUCCESS

First Steps to Success

To succeed in this course, take the following first steps:

- Read the entire Syllabus carefully, making sure that all aspects of the course are clear to you and that you have all the materials required for the course.
- Take time to read the entire Online Student Handbook. The Handbook answers many questions about how to proceed through the course, and how to get the most from your educational experience at Thomas Edison State University.
- Familiarize yourself with the learning management systems environment—how to navigate it and what the various course areas contain. If you know what to expect as you navigate the course, you can better pace yourself and complete the work on time.
- If you are not familiar with web-based learning, be sure to review the processes for posting responses online and submitting assignments before class begins.

Study Tips

Consider the following study tips for success:

- To stay on track throughout the course, begin each week by consulting the Course Calendar. The Course Calendar provides an overview of the course and indicates due dates for submitting assignments, posting discussions, and submitting the final project.
- Check Announcements regularly for new course information.

COMMITMENT TO DIVERSITY, EQUITY, AND INCLUSION

Thomas Edison State University recognizes, values, and relies upon the diversity of our community. We strive to provide equitable, inclusive learning experiences that embrace our students' backgrounds, identities, experiences, abilities, and expertise.

ACCESSIBILITY AND ACCOMMODATIONS

Thomas Edison State University recognizes disability as a facet of diversity and seeks to advance access to its educational offerings. Students with disabilities may seek accommodations by contacting the Office of Student Accessibility Services via email at ada@tesu.edu or phone at (609) 984-1141, ext. 3415. Individuals who are deaf or hard of hearing may call the TTY line at (609) 341-3109.

ACADEMIC POLICIES

To ensure success in all your academic endeavors and coursework at Thomas Edison State University, familiarize yourself with all administrative and academic policies including those related to academic integrity, course late submissions, course extensions, and grading policies.

For more, see:

- University-wide policies
- Undergraduate course policies and regulations
- Graduate academic policies
- Nursing student policies
- Academic code of conduct