CYBR 510: CYBERSECURITY INFORMATION SYSTEMS MANAGEMENT

SYLLABUS FALL 2024

COURSE INFORMATION AND OVERVIEW

Course number and name: CYBR 510, Cybersecurity Information Systems Management
CRNs: 85031 and 87379, 3 credits.
Class meets : Asynchronous
Course Materials: All material is posted on eCampus (https://ecampus.wvu.edu) .
Prerequisite: Acceptance into the MS CYBR Program, PR or CONC: CYBR 530 – Business Data Communications. Exception to course prerequisites may be made by the CYBR Program Coordinator.

Required Textbook:
Kegerreis, M., Schiller, M., and Davis, C. (2020). *IT Auditing Using Controls to Protect Information Assets.* 3rd Edition. McGraw-Hill.
Note: Can be accessed for free on O'reilly using WVU login.
(https://learning.oreilly.com/library/view/it-auditing-using/9781260453232/)

Optional Instructional Materials:

Selected publications of relevance.

For students interested in taking the Certified Information Systems Auditor (CISA) Certification:
Gregory, P.H. (2019). *CISA Certified Information Systems Auditor All-in-One Exam Guide.* 4th Edition. McGraw-Hill. Available on O'reilly (https://learning.oreilly.com/library/view/cisa-certified-information/9781260458817/)

INSTRUCTOR INFORMATION

Instructor: Mohammad (MJ) Ahmad Ph.D.,

Email: mohammad.ahmad@mail.wvu.edu (Emails sent to @mix.wvu.edu account will be ignored). The best and preferred method of communication is via Email.

Office location: 2109 Reynolds Hall. **Tel:** +1(304)293-7939

Office hours: Online office hours TR 10:00AM – 12:00PM., please use the Schedule Appointment link to schedule an appointment. If you wish to meet at other times, please email Dr. Ahmad.

Additional and optional channel of communication: Zoom if needed.

COURSE DESCRIPTION

The course will provide Business Cybersecurity Management (CYBR) students with an overview of the information technology (IT) audit function from an information systems administration perspective. This course will examine in detail how to build and manage an effective IT audit operation capable of analyzing, assessing, and evaluating physical, technical, and operational cybersecurity controls on network architecture, databases, operating systems, applications, storage, endpoints, and cloud computing environments, using information systems auditing standards and frameworks such as COBIT, ISO, and ITIL.

COURSE LEARNING OUTCOMES

This course focuses on the technical and managerial aspects of information systems auditing and systems administration. The lectures, labs, and business cases are designed to explore the IT audit process. At the end of the course, the student should:

1. Demonstrate via testing that the student has a good understanding of the IT audit process
2. Be able to assess and audit applications, databases, network architectures, operating systems, storage, endpoints, and cloud computing environments to find potential information system security control weaknesses through a series of hands on lab assignments.
3. Demonstrate in writing knowledge of effective auditing techniques of a variety of enterprise IT systems, networks, and environments
4. Demonstrate via testing knowledge of IT auditing frameworks, standards, regulations, and the risk management life cycle.

ADDITIONAL BENEFITS OF CLASS: After completion of this course, the student should be able to do additional study and sit for the Certified Information Systems Auditor (CISA) Certification. Taking or passing the CISA is in no way a requirement of this class. However, if a student successfully passes the exam, they will be automatically awarded a 100% on the final exam.

ASSESSMENTS

The online lectures, online class discussions, online labs and online exams are all designed to explore information security assurance topics, risk management, and compliance.

- Learning. Students are required to read the assigned text, practice IT auditing techniques described in the assigned text, and well as read additional supplemental materials hosted on eCampus

- Discussion. Students are expected to participate in weekly discussion questions which will focus on content covered in weekly modules.

- Homework / Labs. Up-to 5 Homework labs will be assigned throughout this course. Students will be expected to fully complete each assignment. Homework Labs are assigned to each student group., and only one assignment will need to be submitted for each group.

- Tests. There are three tests during the semester as well as a cumulative final exam held during the exam period. The tests will be mostly multiple choice, and will test on material covered in the textbook, the homework labs, as well as any supplementary learning material on eCampus. Tests will be timed but are open book.

- Contribution. Each team member will be evaluated by their fellow team members twice throughout the semester. The first evaluation will occur at the midterm, and the second will be after the submission of the final project. Each member will be asked to assess the overall contribution, participation, responsiveness, and initiative of their teammates in working on the group assessments. Each student is expected to complete one evaluation for each of their group members.

- Group Research Projects. Each team will be required to submit a group project during Module 7. The group research project can be on any IT auditing, systems administration, or systems security topic. The group project does not have to be on a topic we have covered in class, in-fact I encourage groups to explore new cutting-edge topics in the previous mentioned areas. The group project can be a PowerPoint presentation, written paper, annotated video, poster, or other form of presentation. Regardless of the presentation medium, I am looking for projects that take an in-depth look on a topic that demonstrates the group has mastery knowledge over the chosen topic. Each group should have no more than 4 group members.

  Example subjects/topics are as follows*:

  - IT auditing frameworks & standards
  - Cloud security
  - Operating systems security
  - Zero-day attacks
  - Challenges in vulnerability management auditing
  - Enterprise Patch Management

  * You do not have to choose one of these topics, these are merely examples!

GRADES

Performance on graded activities will be recorded in the grade book. Anticipate grades to appear within a week or two following the due date.

- **Grading Scale**: >90% A; 80-89.9% B; 70-79.9% C; 60-69.9% D; <60% F
- Course Grading:

Element	Delivery	Count	Total % of grade
Semester Exams	Individual	3	25
Homework	Team	Up to 5	25
Discussions	Individual	Up to 5	10
Final Project	Team	1	15
Cumulative Final Exam	Individual	1	15
Contribution	Individual/ Team	2	10
TOTAL			100%

CLASS POLICIES

Attendance Policy: There is no residency associated with this course. The course is designed for asynchronous learning. There will be periodic opportunities to meet on-line for supplementary presentations strictly within the confines of the eCampus environment. All such meetings will be archived and made available for later review.

Assessment's submission Policy: Students are responsible for all material covered in the course, keeping track of assignments and examination dates. All materials will be posted on eCampus, and your assessments must be submitted in the expected formats by the given due dates on eCampus, submissions over email are not accepted. Any late work may be rejected without a grade except when a policy indicates otherwise. You should keep secure copies of your work in case of data loss.

Makeup Assignments: I understand life gets in the way of education at times, however, please try to honor the due dates for each assignment. Should outside commitments cause a problem in meeting a due date, contact the instructor to arrange a resolution to the conflict.

Class Meetings and Virtual Meetings: The presentation of this course will occur through asynchronous delivery of course material in the form of eCampus content, annotated slide lectures, activities, and optional videos. The course has been divided into 7 modules. Each module has an opening and a closing

date, functioning as a window in which all lesson material must be completed. The instructor will respond to all student emails during the class session period within 24 hours M-F.

Team-based assessments Policy: In the first week of classes, students will self-select into working groups for the semester. Each group can have up-to 4 group members, please refer to the groups sign-up form on eCampus to create and view groups. Students are expected to collaborate professionally with all group members to submit team-based assessments. For groups to function efficiently and fairly, you may like to find a common time to meet regularly via Zoom by using a website such as Doodle or Calendly. The groups are expected to distribute the work among the group members equally. If there are any issues the arise regarding the groups or group-based assessments, please do reach out to your instructor ASAP.

General Comments: The instructor reserves the right to change this syllabus as time and circumstances dictate.

RELATED STATEMENTS

- Institutional Policies: Students are responsible for reviewing policies (https://tlcommons.wvu.edu/qualitymatters/syllabus-policies-and-statements) on inclusivity, academic integrity, incompletes, sale of course materials, sexual misconduct, adverse weather, as well as student evaluation of instruction, and days of special concern/religious holiday statements.

- The use of generative artificial intelligence: Forms of writing assistance that utilize artificial intelligence (AI) to proofread a student's own written work (such as spellcheck or Grammarly) are acceptable. However, tools that rely on generative AI (such as GPT-3, ChatGPT, and Bard) that actually "write" (or generate) text from a prompt are not to be used to generate drafts or written work for any assignment in this course. If students are unsure which AI tools are acceptable, they should consult the instructor prior to using them.

- Student Evaluation of Instruction: Effective teaching is a primary mission of West Virginia University. Student evaluation of instruction provides the university and the instructor with feedback about your experiences in the course for review and course improvement. Your participation in the evaluation of course instruction is both strongly encouraged and highly valued. Results are strictly confidential, anonymous, and not available to the instructor until after final grades are released by Admissions and Records. Information about how you can complete this evaluation will be provided later. I faithfully read my evaluations and incorporate improvements to our future classes based on useful criticism from your SEI's, so please be sure to complete these forms.

- Instructor Access: I am always happy to meet with you then, or else any time that is mutually convenient by appointment. It is easy for me to set up a Zoom for a video chat that meets with your convenience. You are always welcome to email me with questions or to arrange a meeting. I will always respond to your emails within 24 hours, Monday through Friday. If you choose to email me,

please always include the course number in the title of your email and which assessment/ issue you are reaching out about. For example, if you have a question regarding HW 2, please use something like this in your email title "CYBR510- HW #2 question". If your email relates to a team-based assessment, please make sure you always include your group number in your email. I enjoy meeting with students during my office hours, am also happy to discuss possible research and collaboration research in any cybersecurity topics, or any issues which are important to you about the class.

USEFUL LINKS

- 2024-2025 Academic Calendar
- Final Exams calendar

For more information on West Virginia University's Diversity, Equity, and Inclusion initiatives, please see WVU's diversity page.

EXPECTED TIMELINE

The following schedule is an estimate schedule of the topics covered in this class along with the designated week. This might change depending on the progress of students in the class.

Week #	Date	Text Chapter(s)	Topic	Deliverables and Due Dates
1	8/21-8/25	Chapter 1	Introduction to IT Audit Function	Group Sign-Up Introductory Discussion Question Policy acknowledgment survey (DUE 8/25)
2	8/26- 9/1	Chapter 2	Overview of the Audit Process	Exam 1: Chapters 1, 2 (DUE 9/1) Discussion 1 (DUE 9/1) Homework 1 (DUE 9/1)
3	9/2- 9/8	Chapters 3-6	Auditing Controls, Cybersecurity Programs, Data Centers, Disaster Recovery, and Networks	Discussion 2 (DUE 9/8) Homework 2 (DUE 9/8)
4	9/9- 9/15	Chapters 7-10	Server Auditing, Operating Systems, Web Servers, Web Applications, and Databases Server Auditing, Operating Systems, Web Servers, Web Applications, and Databases	Exam 2: Chapters 3 – 10 (DUE 9/15) Discussion 3 (DUE 9/15) Homework 3 (DUE 9/15)
5	9/16-9/22	Chapters 11-13	Auditing Data Storage Environments	Discussion 4 (DUE 9/22) Homework 4 (DUE 9/22)
6	9/23-9/29	Chapters 14-18	Auditing Endpoints, Applications, Cloud Environments, and Projects	Exam 3: Chapters 11 – 18 (DUE 9/29) Discussion 5 (DUE 9/29) Homework 5 (DUE 9/29)
7	9/30-10/6	Chapters 19-21	Frameworks, Standards, Regulations, and Risk Management	Work on Projects Final Project (DUE 10/6)
8	10/7-10/10	All Chapters	10/10 Last day and Final Exam	Cumulative Final Exam Taking and passing the CISA Certification exam will count as an automatic 100% on the Final Exam