## **CYBR 482: Information Technology Audit and Control (3 credits)**

This course introduces the principles and practices of auditing and controlling information technology systems. The course covers the legal, ethical, and regulatory aspects of IT auditing and control, as well as the tools and techniques used by IT auditors and control professionals. ***(****Prerequisite****:*** *CYBR 310****)***

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate critical understanding of the principles and practices of auditing and controlling information technology systems.

A2. Apply auditing principles and practices using various tools and techniques for comprehensive IT system assessments.

B1. Proficiently use audit methodologies, tools, and techniques employed in assessing and ensuring compliance with security standards.

B2. Evaluate the effectiveness of IT audits by critically analyzing findings, identifying areas for improvement, and proposing solutions.

B3. Effectively communicate IT audit results, both in written reports and oral presentations, ensuring clarity and understanding among stakeholders.

C1. Demonstrate effective teamwork and collaboration skills in the context of security audits, working collaboratively to address complex security challenges.

C2. Integrate legal and ethical considerations into IT auditing and control practices, ensuring responsible and compliant IT operations.

**Course Learning Materials:**

* Mike Schiller, Chris Davis, Mike Kegerreis , IT Auditing Using Controls to Protect Information Assets, 3rd Edition, McGraw-Hill, 2019
* William Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards, 1st edition, 2019, pearson

**Course Content:**

1. Building an Effective Internal IT Audit Function
2. Auditing Cybersecurity Programs
3. Auditing Data Centers and Disaster Recovery
4. Auditing Networking Devices
5. Auditing Windows Servers, Auditing Unix and Linux Operating Systems
6. Auditing Web Servers and Web Applications
7. Auditing Big Data and Data Repositories
8. Auditing Storage
9. Auditing Virtualized Environments
10. Auditing End-User Computing Devices
11. Auditing Applications
12. Auditing Cloud Computing and Outsourced Operations
13. Frameworks, Standards and Regulations