CENTRAL TEXAS COLLEGE  
ITSY 2459  
SECURITY ASSESSMENT AND AUDITING  

Semester Hours Credit: 4

INSTRUCTOR: ____________________________

OFFICE HOURS: __________________________

I. INTRODUCTION

   A. Comprehensive experience for the security curriculum. Synthesizes technical material covered in prior courses to monitor, audit, analyze, and revise computer and network security systems to ensure appropriate levels of protection are in place to assure regulatory compliance.

   B. This course serves as a required or elective course on various degree plans. Curriculum plans for degrees and certificates are listed in the current Central Texas College catalog.

   C. The delivery method of this course may be traditional lecture/lab, blended lecture/lab, or online.

   D. Prerequisites: Twelve (12) semester hours of Information Technology Security (ITSY) coursework.

II. LEARNING OUTCOMES

   Upon successful completion of this course, Security Assessment and Auditing, the student will be able to:

   A. Evaluate security plan to ensure appropriate level of protection. (C5, C6, C8, C15, C19, C20).

   B. Assess network security design. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

   C. Audit network system based on security design. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

   D. Use relevant tools to assure security requirements. (C5, C6, C8, C15, C19, C20).

   E. Review all security policies and procedures on a regular basis. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

December 2018
III. INSTRUCTIONAL MATERIALS

A. The instructional materials identified for this course are viewable through www.cted.edu/books

B. Lecture Classes also require at least one USB storage device. Online students may use cloud-based storage.

IV. COURSE REQUIREMENTS

A. Attend both lecture and lab or in the case of online delivery, be actively engaged in Blackboard and maintain constant progress.

B. Be prepared to participate in discussion, team projects/assignments and take unannounced assessments relating to the lecture materials.

C. Complete all exams/assessments.

D. Submit all assignments on time.

V. ASSESSMENTS

A. Student content mastery will be evaluated in the following areas:
   • Assessments (midterm exam, quizzes, projects, discussion etc.)
   • Final Assessment (final exam and/or semester project, participation)

B. Scheduled and unscheduled assessments will be given at the discretion of the instructor.

C. Exams/assessments may be composed of both subjective and objective questions plus computer output.

D. A student must take all exams/assessments. Both online and on campus students who know in advance that they will be absent due to school sponsored trips, military duty or orders, or any other valid reason, must arrange to take an early exam/assessment. Unexpected absences due to illness or other extenuating circumstances will require the student to contact the instructor about make-up work in lieu of the missed exam/assessment.

E. Students with unexcused absences will be given a zero for each missed assignment.
VI. SEMESTER GRADE COMPUTATION

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Points</th>
<th>Points</th>
<th>Grade</th>
<th>Quality Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>300</td>
<td>900</td>
<td>A-Superior</td>
<td>4</td>
</tr>
<tr>
<td>Assessments</td>
<td>300</td>
<td>800-899</td>
<td>B-Above Average</td>
<td>3</td>
</tr>
<tr>
<td>Final Assessment</td>
<td>400</td>
<td>700-799</td>
<td>C-Average</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
<td>600-699</td>
<td>D – Passing but Unsatisfactory</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0-599</td>
<td>F-Failure</td>
<td>0</td>
</tr>
</tbody>
</table>

VII. NOTES AND ADDITIONAL INSTRUCTIONS FROM THE INSTRUCTOR

A. Information on the following Academic Policies, as described in the CTC Course Catalog will be followed:
   1. Withdrawals
   2. Grading
   3. Class Attendance and Course Progress
   4. Scholastic Honesty

B. Cell Phones and Pagers: Students will silence cell phones and mobile devices while in the classroom or lab.

C. Americans with Disabilities Act (ADA): Disability Support Services provide services to students who have appropriate documentation of a disability. Students requiring accommodations for class are responsible for contacting the Office of Disability Support Services (DSS) located on the central campus. This service is available to all students, regardless of location. Review the website at [www.ctcd.edu/disability-support](http://www.ctcd.edu/disability-support) for further information. Reasonable accommodations will be given in accordance with the federal and state laws through the DSS office.

D. Instructor Discretion: The instructor reserves the right of final decision in course requirements and may make changes to the course outline and/or assignments as needed.

E. Civility: Individuals are expected to be aware of what a constructive educational experience is and be respectful of those participating in a learning environment. Failure to do so can result in disciplinary action up to and including expulsion.
VIII. COURSE OUTLINE

A. Lesson One: Information Security Compliance and Compliance Laws

1. Learning Outcomes: Upon successful completion of this lesson the student will be able to:
   a. Examine the role of an IT assessment.
   b. Examine the role of IT auditing.
   c. Compare the differences between an audit and an assessment.
   d. Summarize compliance and explain why it is important.
   e. Describe the goals and requirements for key acts of Congress.
   f. Recall the Department of Defense requirements and the importance of information assurance.
   g. Describe the goals and requirements of the Payment Card Industry Data Security Standard.
   h. Describe various regulations concerning protection of health, accounting, and other information.

2. Learning Activities
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. Lesson Outline: Follow the sequence of lesson objectives.

B. Lesson Two: Information Security Compliance Audit—Standards and Framework

1. Lesson Objectives: Upon successful completion of this lesson the student will be able to:
   a. Recall what organizations need to do to achieve and maintain compliance.
   b. Explain why protecting privacy data is important for achieving compliance.
   c. Review the process for selecting security controls.
   d. Compare the different domains of IT infrastructure.
   e. Recall the importance in using a framework for audits.
   f. Describe various strategies for using standards and framework for compliance auditing.
   g. Review the COSO and how it relates to information technology.
   h. Describe the key parts and importance of COBIT.
   i. Recall the importance and benefits of a SAS 70 audit.
   j. Describe the key ISO/IEC standards that relate to information security.
   k. Describe the NIST 800-53 and 800-53A standards.
   l. Recall the need for hybrid auditing approaches.

2. Learning Activities
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)

c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. **Lesson Outline**: Follow the sequence of lesson objectives.

C. **Lesson Three**: Planning an IT Infrastructure Audit for Compliance

1. **Learning Outcomes**: Upon successful completion of this lesson the student will be able to:
   a. Understand how to define the scope and frequency of an audit.
   b. Identify the key requirements for an audit.
   c. Understand the importance of risk management in assessing security controls.
   d. Understand information and resources needed for an IT audit.
   e. Relate the IT security policy framework into the seven domains of IT infrastructure.
   f. Understand why monitoring requirements help with an IT audit.
   g. Identify security control points.
   h. Differentiate between the project management tasks of an IT audit.

2. **Learning Activities**
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. **Lesson Outline**: Follow the sequence of lesson objectives.

D. **Lesson Four**: Conducting an IT Infrastructure Audit for Compliance and Writing the IT Infrastructure Audit Report

1. **Learning Outcomes**: Upon successful completion of this lesson the student will be able to:
   a. Explain the elements of conducting an audit of IT infrastructure.
   b. Recognize strategies to manage risk and provide baseline configurations to control risk.
   c. Recall why conducting a gap analysis is important.
   d. Recognize when it is necessary to conduct an audit taking a layered approach.
   e. Evaluate different methods and techniques for performing an IT security assessment.
   f. Explain how a security assessment fits into the audit process.
   g. Identify different types of tools used to enable an audit.
   h. Recognize the value of monitoring and configuration management to the audit process.
i. Recall a methodology to testing security controls.
j. Identify common issues that might hamper the audit efforts.
k. Recognize safeguards necessary for security operations and administration roles.
l. Design the layout for a proper executive summary.
m. Recall audit findings and their importance to the audit report.
n. Explain the gap analysis and its importance to the audit report.
o. Identify the risk components part of an IT security assessment and audit report.
p. Recognize how IT security controls identified in the IT audit report relate to the security policy framework and protection of privacy data.
q. Identify key areas from which a gap analysis should be documented.
r. Recall how to report upon a compliance assessment.
s. Recall how to craft meaningful compliance recommendations.

2. Learning Activities
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. Lesson Outline: Follow the sequence of lesson objectives.

E. Lesson Five: Compliance within the User Domain, Workstation, and LAN Domains

1. Learning Outcomes: Upon successful completion of this lesson the student will be able to:
   a. Examine compliance law requirements and business drivers.
   b. Compare how items found in the User Domain contribute to compliance.
   c. Describe methods of ensuring compliance in the User Domain.
   e. Compare how devices and components found in the Workstation Domain contribute to compliance.
   f. Describe methods of ensuring compliance in the Workstation Domain.
   g. Summarize best practices for Workstation Domain compliance.
   h. Compare how devices and components found in the LAN Domain contribute to compliance.
   i. Describe methods of ensuring compliance in the LAN Domain.
   j. Summarize best practices for LAN Domain compliance.

2. Learning Activities
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. Lesson Outline: Follow the sequence of lesson objectives.
F. **Lesson Six:** Compliance within the LAN-to-WAN and WAN Domains

1. **Learning Outcomes:** Upon successful completion of this lesson the student will be able to:
   a. Examine compliance law requirements and business drivers.
   b. Compare how devices and components found in the LAN-to-WAN Domain contribute to compliance.
   c. Describe methods of ensuring compliance in the LAN-to-WAN Domain.
   e. Compare how devices and components found in the WAN Domain contribute to compliance.
   f. Describe methods of ensuring compliance in the WAN Domain.
   g. Summarize best practices for WAN Domain compliance requirements.

2. **Learning Activities:**
   a. Read and discuss chapter (C5, C6, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. **Lesson Outline:** Follow the sequence of lesson objectives.

G. **Lesson Seven:** Compliance within the Remote Access and System/Application Domains

1. **Learning Outcomes:** Upon successful completion of this lesson the student will be able to:
   a. Examine compliance law requirements and business drivers.
   b. Compare how devices and components found in the Remote Access Domain contribute to compliance.
   e. Compare how devices and components found in the System/Application Domain contribute to compliance.
   f. Describe methods of ensuring compliance in the System/Application Domain.
   g. Summarize best practices for System/Application Domain compliance.

2. **Learning Activities:**
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. **Lesson Outline:** Follow the sequence of lesson objectives.
H. **Lesson Eight:** Ethics, Education, and Certification for IT Auditors

1. **Learning Outcomes:** Upon successful completion of this lesson the student will be able to:
   a. Understand the required skills and knowledge required for a career in IT auditing.
   b. Understand what makes up a code of conduct and a code of ethics.
   c. Identify codes of ethics from various professional organizations.
   d. Identify the components that make up a mature code of conduct and why organizations establish them.
   e. Understand the differences between auditing associations and other professional bodies.
   f. Differentiate between certifications available to auditors and IT professionals.
   g. Identify educational opportunities and resources available to IT auditors.

2. **Learning Activities:**
   a. Read and discuss chapter (C5, C6, C8, C19, F1, F5, F11)
   b. Complete assigned case studies (C5, C6, C8, C19, F1, F5, F11)
   c. Complete exercises (C5, C6, C8, C19, F1, F5, F11)

3. **Lesson Outline:** Follow the sequence of lesson objectives.