Credit Hours: 3

Contact Hours: This is a 3-credit course, offered in accelerated format. This means that 16 weeks of material is covered in 8 weeks. The exact number of hours per week that you can expect to spend on each course will vary based upon the weekly coursework, as well as your study style and preferences. You should plan to spend 14-20 hours per week in each course reading material, interacting on the discussion boards, writing papers, completing projects, and doing research.

COURSE DESCRIPTION AND OUTCOMES

COURSE DESCRIPTION:

ITS350 provides students with the skills and knowledge required to support IT security, planning, and cryptology in organizational settings. The course also prepares the student for the Testout Security Pro and CompTIA Security + certifications.

COURSE OVERVIEW:

This course enhances students’ skills in the area of security, planning, cryptology, and security technologies. Prepares students for CompTIA Security+ certification exam. Recommended Prior Course: ITS310 or ITS315.

COURSE LEARNING OUTCOMES:

1. Analyze an organization’s network security needs and potential vulnerabilities.
2. Employ viable solutions to meet the security needs of an organization.
3. Demonstrate working knowledge of network security concepts, issues, vulnerabilities, and required planning for industry network security concerns.
4. Use assessments and lab simulations to prepare for the Security + exam.
5. Apply tools, conceptual knowledge, and concrete skills to align organizational needs with Information Technology initiatives for a secure network environment.

PARTICIPATION & ATTENDANCE

Prompt and consistent attendance in your online courses is essential for your success at CSU-Global Campus. Failure to verify your attendance within the first 7 days of this course may result in your withdrawal. If for some reason you would like to drop a course, please contact your advisor.

Online classes have deadlines, assignments, and participation requirements just like on-campus classes. Budget your time carefully and keep an open line of communication with your instructor. If you are having technical
problems, problems with your assignments, or other problems that are impeding your progress, let your instructor know as soon as possible.

**COURSE MATERIALS**

Textbook Information is located in the CSU-Global Booklist on the Student Portal.

**COURSE SCHEDULE**

Due Dates

The Academic Week at CSU-Global begins on Monday and ends the following Sunday.

- **Discussion Boards:** The original post must be completed by Thursday at 11:59 p.m. MT and peer responses posted by Sunday 11:59 p.m. MT. Late posts may not be awarded points.
- **Critical Thinking:** Assignments are due Sunday at 11:59 p.m. MT.

**WEEKLY READING AND ASSIGNMENT DETAILS**

**MODULE 1**

Readings

- LabSim Security Pro - Chapter 3: Policies, Procedures, and Awareness (Read and view **ALL** content).

**Discussion (25 points)**

**Critical Thinking (60 points)**

**Respond to Social Engineering**

Complete the LabSim lab simulation **3.5.5 – Respond to Social Engineering**.

The lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the assignment. *Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.*

**MODULE 2**

Readings

- LabSim Security Pro - Chapter 4: Physical (Read and view **ALL** content).
Mizroch, A. (2015, Dec 10). In Belgium, an encryption powerhouse rises; University of Leuven has become a battleground in the fight between privacy and surveillance. Wall Street Journal (Online).

Discussion (25 points)

Critical Thinking (60 points)

Implement Physical Security
Complete the LabSim lab simulation 4.1.4 – Implement Physical Security.

Each lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the complete assignment. Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.

Module 3

Readings

- LabSim Security Pro - Chapter 5: Perimeter - Chapter 6: Network (Read and view ALL content).

Discussion (25 points)

Critical Thinking (60 points)

Configure a DMZ and Implement Intrusion Prevention
Complete the LabSim lab simulations:

- 5.4.3 – Configure a DMZ
- 6.8.6 – Implement Intrusion Prevention

Each lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the complete assignment. Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.

PORTFOLIO PROJECT MILESTONE

Submit your Portfolio Topic to your instructor for preliminary approval. Provide reasons for your choice. Your submission should contain no more than one page of content, framed by a cover page and references page.

Module 4
Readings

- LabSim Security Pro - Chapter 6: Network (Read and view ALL content).

Discussion (25 points)

Critical Thinking (60 points)

Vulnerability Assessment
Complete the following LabSim lab simulations:

- 6.9.5 – Scan for Vulnerabilities 1
- 6.9.6 – Scan for Vulnerabilities 2

Each lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the complete assignment. *Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.*

Module 5

Readings

- LabSim Security Pro - Chapter 7: Host - Chapter 8: Applications (Read and view ALL content).

Discussion (25 points)

Critical Thinking (60 points)

Manage Services with Group Policy and Implement Data Execution Preventions
Complete the following LabSim lab simulations:

- 7.4.5 – Manage Services with Group Policy
- 8.6.8 – Implement Data Execution Preventions

Each lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the complete assignment. *Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.*
Module 6

Readings

- LabSim Security Pro - Chapter 8: Application (Read and view ALL content).

Discussion (25 points)

Critical Thinking (70 points)

Restrict Local Accounts and Secure Default Accounts

Complete the following LabSim lab simulations:

- 8.13.7 – Restrict Local Accounts
- 8.13.8 – Secure Default Accounts

Each lab simulation will be graded automatically on a percent basis (100 possible points), which your instructor will convert to 50 points for the complete assignment. **Note that you can re-work each graded lab simulation as many times as you like, so if you repeat each simulation until you get a score of 100%, you can earn a perfect score on every Critical Thinking assignment.**

Module 7

Readings

- LabSim Security Pro - Chapter 9: Data (Read and view ALL content).

Discussion (25 points)

Module 8

Readings

- LabSim Security Pro - Chapter 9: Data (Read and view ALL content).
Discussion (25 points)

Final Exam (100 points)

Complete the Security Pro Exam, which can be accessed from your Home page in LabSim, before midnight of week 8. You can only take this exam once.

Portfolio Project (250 points)

Choose one of the following two Portfolio Project options to complete by the end of Week 8. Do not do both assignments. Identify your assignment choice in the title of your submission. When you are ready to submit, click the Week 8 Portfolio Project header on the Assignments page to upload the document.

OPTION #1: XYZ Corporation

XYZ Corporation is a small organization of roughly 20 to 30 employees working in a simple office space using basic peer-to-peer type networking in which all employees keep their data on their own PCs and each has his or her own devices (i.e., printers, scanners, and other peripherals).

In the last few months, XYZ developed a revolutionary widget that will change technology as we know it. The company received a substantial investment and will quickly ramp up to 100 employees. They moved into a new building that was wired and set up for a local area network (LAN). They have implemented a client server-based network in which all printers, folders, and other resources are shared but everyone has access to everything and there is no security outside of the defaults in place when the system was set up.

You have been hired to secure XYZ Inc’s network and ensure that the company has the highest levels of security to prevent internal or external attacks. In an 8-10 page proposal, address the following items to provide a comprehensive secure environment:

1. A plan to provide secure Access Control Methods for all user access
2. A viable Password policy, which includes complexity, duration, and history requirements
3. A cryptography method to ensure vital data is encrypted
4. A remote access plan to ensure that users that access the network remotely do so in a secure and efficient manner
5. A thorough plan to protect the network from Malware and other Malicious attacks

Your proposal should address all of the elements noted above with support, detail, and elaboration for each section explicitly grounded in knowledge from the assigned readings and media, along with any outside sources you may choose to bring into your writing. Your paper should be 8-10 pages in length, conform to CSU-Global Guide to Writing and APA, and include 3-5 scholarly references in addition to the course textbook to support your views. The CSU-Global Library is a good place to find these references.

OPTION #2: ABC Corporation

ABC Corporation is a small but global organization of roughly 200 to 250 employees working in a work-at-home type of office space around the world using Wide Area Network connectivity via VPNs. The company deals with lot of financial information to be shared between the offices that requires encrypted traffic as well as data-at-rest encryption.
You have been hired to secure ABC Inc’s network and ensure that the company has the highest levels of security to prevent internal or external attacks. In an 8-10 page proposal, address the following items to provide a comprehensive secure environment:

1. A plan to provide secure Access Control Methods for all user access
2. A viable Password policy, which includes complexity, duration, and history requirements
3. A cryptography method to ensure vital data is encrypted, including recommendation on algorithms
4. A VPN recommendation to access the network remotely do so in a secure and efficient manner

Your proposal should address all of the elements noted above with support, detail, and elaboration for each section explicitly grounded in knowledge from the assigned readings and media along with any outside sources you may choose to bring into your writing. Your paper should be 8-10 pages in length, conform to CSU-Global Guide to Writing and APA, and include 3-5 scholarly references in addition to the course textbook to support your views. The CSU-Global Library is a good place to find these references.
Course Grading

20% Discussion Participation
37% Critical Thinking Assignments
43% Final Portfolio Project

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>95.0 – 100</td>
</tr>
<tr>
<td>A-</td>
<td>90.0 – 94.9</td>
</tr>
<tr>
<td>B+</td>
<td>86.7 – 89.9</td>
</tr>
<tr>
<td>B</td>
<td>83.3 – 86.6</td>
</tr>
<tr>
<td>B-</td>
<td>80.0 – 83.2</td>
</tr>
<tr>
<td>C+</td>
<td>75.0 – 79.9</td>
</tr>
<tr>
<td>C</td>
<td>70.0 – 74.9</td>
</tr>
<tr>
<td>D</td>
<td>60.0 – 69.9</td>
</tr>
<tr>
<td>F</td>
<td>59.9 or below</td>
</tr>
</tbody>
</table>
IN-CLASSROOM POLICIES

For information on late work and incomplete grade policies, please refer to our In-Classroom Student Policies and Guidelines or the Academic Catalog for comprehensive documentation of CSU-Global institutional policies.

Academic Integrity
Students must assume responsibility for maintaining honesty in all work submitted for credit and in any other work designated by the instructor of the course. Academic dishonesty includes cheating, fabrication, facilitating academic dishonesty, plagiarism, reusing /repurposing your own work (see CSU-Global Guide to Writing and APA Requirements for percentage of repurposed work that can be used in an assignment), unauthorized possession of academic materials, and unauthorized collaboration. The CSU-Global Library provides information on how students can avoid plagiarism by understanding what it is and how to use the Library and Internet resources.

Citing Sources with APA Style
All students are expected to follow the CSU-Global Guide to Writing and APA Requirements when citing in APA (based on the APA Style Manual, 6th edition) for all assignments. For details on CSU-Global APA style, please review the APA resources within the CSU-Global Library under the “APA Guide & Resources” link. A link to this document should also be provided within most assignment descriptions in your course.

Disability Services Statement
CSU-Global is committed to providing reasonable accommodations for all persons with disabilities. Any student with a documented disability requesting academic accommodations should contact the Disability Resource Coordinator at 720-279-0650 and/or email ada@CSUGlobal.edu for additional information to coordinate reasonable accommodations for students with documented disabilities.

Netiquette
Respect the diversity of opinions among the instructor and classmates and engage with them in a courteous, respectful, and professional manner. All posts and classroom communication must be conducted in accordance with the student code of conduct. Think before you push the Send button. Did you say just what you meant? How will the person on the other end read the words?

Maintain an environment free of harassment, stalking, threats, abuse, insults, or humiliation toward the instructor and classmates. This includes, but is not limited to, demeaning written or oral comments of an ethnic, religious, age, disability, sexist (or sexual orientation), or racist nature; and the unwanted sexual advances or intimidations by email, or on discussion boards and other postings within or connected to the online classroom. If you have concerns about something that has been said, please let your instructor know.