Colorado State University GLOBAL CAMPUS

ISM550: INFORMATION SYSTEMS AND SECURITY

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.

Faculty Information: Faculty contact information and office hours can be found on the faculty profile page.

COURSE DESCRIPTION AND OUTCOMES

COURSE DESCRIPTION:

This course presents a broad overview of possible issues and dangers that can compromise information systems in the workplace. Students learn the roles, responsibilities, and essential tools needed for IT Managers to secure an organization's data and operations.

COURSE OVERVIEW:

This course presents an overview of techniques for approaching information security from a management perspective. Topics include administrative and technical security controls to prevent, detect, respond to, and recover from cyber-attacks; risk and vulnerability analysis to select security controls; security planning; security architecture; security evaluation and assessment; and legal, ethical, and privacy aspects of information assurance.

In this course, you will gain fundamental security knowledge, such as risk analysis procedures, cryptography authentication, access control techniques, and their use in network, operating system, database, and application layers. Security issues of current importance are stressed. You will be able to understand the importance of using standards and protocols defined by various agencies such as the National Institute of Standards and Technology (NIST) and the Department of Defense (DoD).

COURSE LEARNING OUTCOMES:

1. Apply risk assessment methodology for selecting security controls to protect information asset.
2. Develop elements of information security management artifacts.
3. Apply layered and defense-in-depth security architecture strategy to deny, deter, deflect, delay and detect attacks.
4. Assess information security techniques in application, operating system, database and network components of information systems.
5. Determine strategy of access control tools and techniques for implementing the security requirements in a cost-effective manner.

6. Examine legal, ethical and privacy aspects associated with information systems and information assurance.

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

Required:

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). NY: Pearson. ISBN13: 9780134794105

NOTE: *All non-textbook required readings and materials necessary to complete assignments, discussions, and/or supplemental or required exercises are provided within the course itself. Please read through each course module carefully.*

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

- Join Taskforce Transformation Initiative, U.S. Department of Commerce, National Institutes of Standards and Technology. (2012) *Guide for conducting risks* (Publication No. SP 800-30 Rev. 1).
- Shin, J., Son, H., Khalil ur, R., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety, 134*, 208-217.

Discussion (25 points)

MODULE 2

Readings

- Chapter 13 in *Computer Security: Principles and Practic*e

Discussion (25 points)

Critical Thinking (100 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: CIA Triad Analysis

Upper management has asked you to provide an analysis of information security technologies specifically related to Confidentiality, Integrity and Availability, along with trusted computing. Your paper should demonstrate that you are able to understand and apply these common information security concepts and must include an analysis that addresses the breadth and coverage of information security regarding people, processes, and technologies.

Your well-developed analysis must meet the following requirements.

- Include four to six pages, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing & APA Requirements. Include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. A percentage of your grade depends on the quality of your writing. If you need assistance with your writing style, start Writing Center in the Library.
- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Rubric in Module 2 for assignment expectations.

Option 2: CIA Triad Presentation

Assume you are the instructor for this class. Prepare a slide presentation in which you discuss information security technologies specifically related to Confidentiality, Integrity and Availability, along with trusted computing.

Your well-developed presentation must meet these requirements.

- Eight or more slides of easy-to-understand content (text and visuals). Avoid distracting transition elements and animations.

- Speaker's notes containing 50-100 words per slide to elaborate on the slide content. Support your notes with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Follow the CSU-Global Guide to Writing & APA Requirements.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Writing Center in the Library.
- Refer to the Rubric in Module 2 for assignment expectations.

MODULE 3

Readings

· Chapter 2 in *Computer Security: Principles and Practice*

Discussion (25 points)

Critical Thinking (100 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: Cryptographic Tools

You work for an organization that is in the defense-contracting field. The federal government audited your organization, as part of doing business with it, and you failed to meet the following requirements.

- Web traffic to and from server is in plain text.
- There are some sensitive emails also being sent outside of organizations that are not encrypted.

Your manager has assigned you to remedy the situation. Write a proposal to resolve these issues, identify solutions, and costs.

Your well-developed proposal must meet the following requirements.

- Include four to six pages, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing & APA Requirements. Include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. A percentage of your grade depends on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.
- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Rubric in Module 3 for assignment expectations.

Option 2: Cryptographic Tools Presentation

You work for an organization that is in the defense-contracting field. The federal government audited your organization, as part of doing business with it, and you failed to meet the following requirements.

- Web traffic to and from server is in plain text.

- There are some sensitive emails also being sent outside of organizations that are not encrypted.

Your manager has assigned you to remedy the situation. Prepare a slide presentation in which you outline the steps necessary to address the audit findings above.

Your well-developed presentation must meet these requirements.

- Eight or more slides of easy-to-understand content (text and visuals). Avoid distracting transition elements and animations.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide content. Support your notes with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Follow the CSU-Global Guide to Writing& APA Requirements.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.

Refer to the Rubric in Module 3 for assignment expectations.

MODULE 4

Readings

· Chapters 3 & 4 in *Computer Security: Principles and Practice*

Discussion (25 points)

Portfolio Milestone (50 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: Identify an Organization, Paper

1. Read the Portfolio Project description and rubric in Module 8.
2. Select an organization that has sufficient publicly available information to support a reasonable risk analysis, particularly including threat and vulnerability identification.
3. Create an organization profile that includes:
   - Name and location
   - Management or basic organization structure
   - Industry and purpose (i.e., the nature of its business)
   - Financial information, standing in its industry, reputation
   - Relevant aspects of the company/organization's computing and network infrastructure.
4. Submit a one- to two-page paper about the organization.

Note: Do not try to access more information through social engineering or through attempted cyber-attacks or intrusion attempts. This is a look at how readily available information might be used from a risk management perspective.

Option 2: Identify an Organization, Presentation

1. Read the Portfolio Project description and rubric in Module 8.
2. Select an organization that has sufficient publicly available information to support a reasonable risk analysis, particularly including threat and vulnerability identification.
3. Note the following about the organization
   - Name and location
   - Management or basic organization structure
   - Industry and purpose (i.e., the nature of its business)
   - Financial information, standing in its industry, reputation
   - Relevant aspects of the company/organization's computing and network infrastructure.
4. Submit a four- to eight-slide presentation (use PowerPoint or other slide presentation software) about the organization.

Note: Do not try to access more information through social engineering or through attempted cyber-attacks or intrusion attempts. This is a look at how readily available information might be used from a risk management perspective.

MODULE 5

Readings

· Chapters 6, 10, & 11 in Computer Security: Principles and Practice

Discussion (25 points)

Critical Thinking (125 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: Software Security Report

Your CIO is currently concerned about malware (viruses, worms, Trojan horses, etc.), that could cripple your organization. She asked you to describe the ways in which different malware functions. Provide at least one example demonstrating how a particular virus has affected one or more organizations.

Your well-developed report must meet the following requirements.

- Include four to six pages, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing & APA Requirements. Include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. A percentage of your grade depends on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.
- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Rubric in Module 5 for assignment expectations.

Option 2: Software Security Presentation

Assume you are the instructor for this class. Prepare a slide presentation in which you discuss the various types of malware present in today's computing environment. Be sure to discuss the essential security controls utilized to address malware threats.

Your well-developed presentation must meet these requirements.

- Eight or more slides of easy-to-understand content (text and visuals). Avoid distracting transition elements and animations.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide content. Support your notes with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Follow the CSU-Global Guide to Writing & APA Requirements.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Writing Center in the Library.

Refer to the Rubric in Module 5 for assignment expectations.

MODULE 6

Readings

- Chapter 12 in *Computer Security: Principles and Practice*

Discussion (25 points)

Critical Thinking (125 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: Operating System Security Report

The organization you work for currently lacks operating system security and uses various Windows and Linux systems that run various Enterprise Resource Planning software. Your CIO is concerned that sensitive data on the servers is at risk.

She asks you to write a report detailing a defense in depth approach for securing data on both operating systems. Consider all standards and processes required to secure the various operating systems. Include at least one security control for each layer of defense.

Your well-developed report must meet the following requirements.

- Four to six pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing & APA Requirements. Include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Be clearly and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Writing Center in the Library.
- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Rubric in Module 6 for assignment expectations.

Option 2: Operating System Security Presentation

The organization you work for currently lacks operating system security and uses various Windows and Linux systems that run various Enterprise Resource Planning software. Your CIO is concerned that sensitive data on the servers is at risk.

She asks you to write a report detailing a defense in depth approach for securing data on both operating systems. Consider all standards and processes required to secure the various operating systems. Include at least one security control for each layer of defense.

Your well-developed presentation must meet the following requirements.

- Eight or more slides of easy-to-understand content (text and visuals). Avoid distracting transition elements and animations.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide content. Support your notes with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Follow the CSU-Global Guide to Writing & APA Requirements.
- Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.

Refer to the Rubric in Module 6 for assignment expectations.

MODULE 7

Readings

- Chapter 5 in *Computer Security: Principles and Practice*

Discussion (25 points)

MODULE 8

Readings

- Chapters 17 & 19 in *Computer Security: Principles and Practice*

Discussion (25 points)

Portfolio Project (300 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option 1: Risk Assessment Report

The objective of this assignment is to develop a Risk Assessment Report for an organization including companies and government agencies.

You will conduct the analysis using only public information from the internet, organizational and news reports, journal articles, etc., and information based on judicious, believable extrapolation of that information. Consider the organization's information assets (computing and networking infrastructure), vulnerabilities, and legitimate threats that can exploit those vulnerabilities.

There is a wealth of business-oriented and technical information that can be used to infer likely vulnerabilities and assets for an organization. It is recommended that students select their organizations based at least in part on ease of information gathering, from a public record perspective.

Instructions

(NOTE: You will complete steps 1 and 2 by the end of Week 4 to submit as the Portfolio Project Milestone.)

1. Select an organization that has sufficient publicly available information to support a reasonable risk analysis, particularly including threat and vulnerability identification.
2. Create an organization profile that includes:
   - Name and location
   - Management or basic organization structure
   - Industry and purpose (i.e., the nature of its business)
   - Financial information, standing in its industry, reputation
   - Relevant aspects of the company/organization's computing and network infrastructure

   Note: Do not try to access more information through Social Engineering or through attempted cyber-attacks or intrusion attempts. This is a look at how readily available information might be used from a risk management perspective.

3. Conduct the analysis using the National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems.
   a. Focus on identifying threats and vulnerabilities faced by the organization.
   b. Based on the threats and vulnerabilities, determine the likelihood and severity of impact that would occur should each of the threats materialize. This should produce a listing of risks, at least roughly ordered by their significance to the organization.

c. For the risks you have identified, suggest ways that the subject organization might respond to mitigate the risk.

Your well-developed report must meet the following requirements.

- Include 15 to 20 pages, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing & APA Requirements. Include an introduction, a body, and a conclusion.
- Be clear and employ excellent grammar and style techniques. Be concise. Be logical. A percentage of your grade depends on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.
- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Rubric in Module 8 for assignment expectations.

Option 2: Risk Assessment Report, Presentation

The objective of this assignment is to develop a Risk Assessment Report for an organization including companies and government agencies.

You will conduct the analysis using only public information from the internet, organizational and news reports, journal articles, etc., and information based on judicious, believable extrapolation of that information. Consider the organization's information assets (computing and networking infrastructure), vulnerabilities, and legitimate threats that can exploit those vulnerabilities.

There is a wealth of business-oriented and technical information that can be used to infer likely vulnerabilities and assets for an organization. It is recommended that students select their organizations based at least in part on ease of information gathering, from a public record perspective.

Instructions

(NOTE: You will complete steps 1 and 2 by the end of Week 4 to submit as the Portfolio Project Milestone.)

1. Select an organization that has sufficient publicly available information to support a reasonable risk analysis, particularly including threat and vulnerability identification.
2. Create an organization profile that includes:
    - Name and location
    - Management or basic organization structure
    - Industry and purpose (i.e., the nature of its business)
    - Financial information, standing in its industry, reputation
    - Relevant aspects of the company/organization's computing and network infrastructure

Note: Do not try to access more information through Social Engineering, or through attempted cyber-attacks or intrusion attempts. This is a look at how readily available information might be used from a risk management perspective.

3. Conduct the analysis using the National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems.
   a. Focus on identifying threats and vulnerabilities faced by the organization.
   b. Based on the threats and vulnerabilities, determine the likelihood and severity of impact that would occur should each of the threats materialize. This should produce a listing of risks, at least roughly ordered by their significance to the organization.
   c. For the risks you have identified, suggest ways that the subject organization might respond to mitigate the risk.

Your well-developed report must meet the following requirements.

- Twenty or more slides of easy-to-understand content (text and visuals). Avoid distracting transition elements and animations.
- Speaker's notes containing 300 words or more per slide to elaborate on the slide content. Support your notes with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Follow the CSU-Global Guide to Writing and APA Requirements. Be clear and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with the Writing Center in the Library.

Refer to the Rubric in Module 8 for assignment expectations.

COURSE POLICIES

Course Grading

20% Discussion Participation
45% Critical Thinking Assignments
35% Final Portfolio Project
0% Live Classroom

Grading Scale	
A	95.0 – 100
A-	90.0 – 94.9
B+	86.7 – 89.9
B	83.3 – 86.6
B-	80.0 – 83.2
C+	75.0 – 79.9
C	70.0 – 74.9
D	60.0 – 69.9
F	59.9 or below

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.