Colorado State University GLOBAL CAMPUS

ISM527: CYBER SECURITY MANAGEMENT

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 provides graduates with insight to the complexities with the implementation and management of cyber security in an enterprise. Students will need to perform risk assessments and recommend mitigations to protect digital assets in the workplace. Other topics in this course include: disaster recovery, incident handling, cyber security policy implementation, as well as privacy and legal issues related to cyber security.

COURSE OVERVIEW:

Cyber security has become a topic of critical importance in today's networked and interconnected environment. The study of cyber security management describes the techniques, methods, and strategies used by information security professionals to combat security breaches and threats. This course provides an overview of the field of information security and in-depth knowledge of the complex nature of related threats and countermeasures. Students examine key strategies and methodologies used to increase business continuity and disaster preparedness. Also presented are methods of securing information systems using security controls, policies, and best practices with coverage extended to additional topics including information privacy and information security laws and regulations.

COURSE LEARNING OUTCOMES:

1. Evaluate internal threats, external threats and vulnerabilities to data assets in the enterprise.
2. Provide recommendations to mitigate or eliminate areas of weakness in the enterprise.
3. Identify the requirements to secure the physical perimeter of an enterprise.
4. Discuss social engineering techniques used to compromise digital assets in an enterprise.
5. Develop a comprehensive security assessment for an existing enterprise infrastructure.

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:

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). Boston, MA: Cengage Learning. ISBN 13: 9781035501256

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

- Chapter 1 in *Management of Information Security*
- Alexander, A., & Cummings, J. (2016). *The rise of the chief information security officer*. *People & Strategy, 39*(1), 10-13.

Discussion (25 points)

Critical Thinking (75 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: Analysis of Recent Security Breaches

The text has provided an overview of information security and its importance within an organization. In the digital world that we live in, information security is critical to the success and health of any organization. Any security breach, even a small one, can have devastating consequences.

Using the Internet, find two recent examples of organizations that encountered security breaches, then describe and analyze each, offering a solution that would have prevented the breach. Your answer should account for each of the following items:

1. Provide an overview of the incident.
2. Describe what you believe led to or allowed the breach to occur.
3. Explain what could have been done to prevent this breach.
4. Analyze the situation in detail. If you could go back in time, what changes or things would you have the company do differently to have prevented such an attack? What concepts for this module apply to the security breaches that you identified?

Your paper should be 4-6 pages in length and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

Option #2: Analysis of the Rise of the CIO

In the past, the CIO has been focused internally. However, the rise of the CIO is becoming apparent. The CIO is becoming a key adviser on an organization's strategy. The rise of the CIO coincides with several other trends in the business world over the past few years and the growing importance of technology. Now, the CIO is in the central role for deciding the technology strategy for an organization.

Using the Internet, find at least two trends that are now affecting an organization which have helped cause the rise of the CIO. Your answer should account for each of the following items:

5. Provide an overview of the trends.
6. Describe how these trends affect an organization.
7. Explain how the CIO can decide on the technology strategy for the organization that considers these trends.
8. Lastly, describe the new skill-set requirements of CIOs with this rise.

Your paper should be 4-6 pages in length and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

MODULE 2

Readings

- Chapters 2 & 3 in *Management of Information Security*
- Harper, J. (2018). The critical confluence of information governance and security breaches. *KMWorld*, *27*(2), 10-12.
- Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3-13.

Discussion (25 points)

Critical Thinking (75 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: Analysis of Unethical and Illegal Behavior

The text has provided an overview of laws and ethics and its importance for organizations. In the digital world we live in, ethical behavior is critical to the success and health of any organization. Any unethical or illegal behavior, even something small, can have devastating consequences. Using your readings from this week, answer the following questions for this week's critical thinking activity.

What are the three general categories of unethical and illegal behavior? What is the best method for preventing unethical and illegal behavior?

Discuss and cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find scholarly sources. Your paper should be 4-6 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Review the Critical Thinking grading rubric, found in the Week 2 folder, to see how you will be graded for this assignment.

Option #2: IT Strategic Planning

Review the case at the beginning and end of Chapter 3. Answer questions 1 and 2 in the Closing Case section of the chapter.

Cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find scholarly sources. Your paper should be 4-6 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Review the Critical Thinking grading rubric, found in the Week 2 folder, to see how you will be graded for this assignment.

MODULE 3

Readings

- Chapters 4 & 5 in *Management of Information Security*
- Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71-92.
- Khajouei, H., Kazemi, M., & Moosavirad, S. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems & E-Business Management, 15*(1), 1-19.

Discussion (25 points)

Critical Thinking (75 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: Issue-Specific Security Policy Analysis

Issue-Specific Security Policy (ISSP) provides detailed, targeted guidance to instruct employees in the use of a resource. For this week's critical thinking activity, write a 4- to 6-page paper answering the following questions about ISSP.

What is the purpose of an ISSP? List and describe three functions that an ISSP serves in an organization. What should be the first component of an ISSP when it is presented? Why? What should be the second major component? Why? List and describe three common ways in which ISSP documents are created and/or managed.

Discuss and cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find scholarly sources. Your paper should be 4-6 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Review the Critical Thinking grading rubric, found in the Week 3 folder, to see how you will be graded for this assignment.

Option #2: Security Awareness for CSU-Global

Security awareness programs set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. A security awareness program keeps InfoSec at the forefront of users' minds on a daily basis.

Search for the term "security awareness" on the Internet. Choose one website that offers materials and services for security awareness. Write a 4- to 6-page paper about how you would go about implementing the awareness materials and/or services here at CSU-Global.

Discuss and cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is an excellent place to find scholarly sources. Your paper should be 4-6 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Review the Critical Thinking grading rubric, found in the Week 3 folder, to see how you will be graded for this assignment.

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: Organizational Risk and Security Plan

Develop a brief position paper on the contents of a Business Continuity Plan. Include in your paper your perspectives on the importance of Business Continuity Planning to MDL.

Cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find scholarly sources.

Your paper should be 2-3 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Option #2: Business Impact Analysis

Develop a brief position paper on the contents of a Business Impact Analysis. Include in your paper your perspectives on the importance of a Business Impact Analysis to your selected organization.

Cite the assigned readings from the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is an excellent place to find scholarly sources.

Your paper should be 2-3 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

MODULE 4

Readings

- Chapters 6 & 7 in *Management of Information Security*
- Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2016). Foundations for an intelligence-driven Information security risk-management system. *JITTA: Journal of Information Technology Theory and Application, 17*(3), 25-50.

Discussion (25 points)

Critical Thinking (75 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: Creating a Security Policy

Security policies are common within organizations that focus on providing a secure computing environment. Imagine that you are tasked with drafting a security policy for an organization of your choice.

Using the resources and information provided within this module, draft a 4- to 6-page security policy for an existing or fictitious organization. You have viewed some sample policies at: http://www.sans.org/security-resources/policies/.

In your response, comment on the needs and rationales for each of the following types of policies:

1. Acceptable-Use Policy (AUP)
2. Risk Assessment Policy
3. Remote Access Policy

In your paper ensure that you describe the significance and purpose of the three policy documents listed above and explain how they relate to your selected fictitious organization.

Your response should be 4-6 pages in length, organized, and well-written in conformity with CSU-Global Guide to Writing & APA.

Review the Critical Thinking grading rubric, found in the Week 4 folder, to see how you will be graded for this assignment.

Option #2: Security Vulnerability Exploitation and Tesla

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.

Security vulnerabilities are system bugs, irregularities or other issues that provide mechanisms for exploitation and unintended system use. The larger and more complex a system is, the greater the likelihood that vulnerability exists. Tesla, for example, is a well-recognized player in the automobile industry. Yet in 2016 the company was subject to security hacks as a result of system/device vulnerabilities.

In a 4- to 6-page paper, reply to the following questions regarding the 2016 security breaches experienced by Tesla:

1. What types of security breaches did Tesla face in 2016?
2. What were the economic consequences?
3. What were some non-economic consequences?
4. How were the organization's reputation and brand name affected?
5. What did Tesla do to restore customer confidence and address these security issues?
6. Analyze Tesla's previous and current security practices and evaluate the company's response to this security breach.

Your paper should be 2-4 pages in length, organized, and well-written in conformity with CSU-Global Guide to Writing & APA.

In support of your response, cite and integrate at least two credible outside sources as well as your textbook, for a total of three or more sources. The CSU-Global Library is a great place to find these resources. Place these in a reference page formatted in accordance with APA style. This reference page does not count toward the total page requirement.

Examine the Critical Thinking grading rubric, found in the Week 4 folder, to see how you will be graded for this assignment.

MODULE 5

Readings

- Chapters 8 & 9 in *Management of Information Security*
- Vincent, N. (2016). A holistic approach to IT risk: The COBIT framework can help auditors understand and address their organization's technology risks. *Internal Auditor, 73*(6), 18.

Discussion (25 points)

Critical Thinking (75 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: Comparison of Security Models

Compare the ISO/IEC 27001 outline with the NIST publications discussed in the assigned reading material.

In a 3- to 4-page paper answer the following questions:

1. What areas, if any, are missing from the NIST publications?

2. Identify the strengths and weaknesses of the NIST programs compared to the ISO standard.

Your paper should be organized and well-written in conformity with CSU-Global Guide to Writing & APA.

In support of your response, cite and integrate at least two credible outside sources as well as your textbook, for a total of three or more sources. The CSU-Global Library is a great place to find these resources. Place these in a reference page formatted in accordance with APA style. This reference page does not count toward the total page requirement.

Review the Critical Thinking grading rubric, found in the Week 5 folder, to see how you will be graded for this assignment.

Option #2: Access Control Analysis

Access Controls regulate the admission of users into trusted areas of the organization. They are comprised of four elements. For this week's critical thinking activity, write a 4- to 6-page paper answering the following questions:

1. What are the essential processes of access control?
2. What are the key principles on which access control is founded?
3. Identify at least two approaches used to categorize access control methodologies and list the types of controls found in each.
4. What is mandatory access control?

Your paper should be organized and well-written in conformity with CSU-Global Guide to Writing & APA.

In support of your response, cite and integrate at least two credible outside sources as well as your textbook, for a total of three or more sources. The CSU-Global Library is a great place to find these resources. Place these in a reference page formatted in accordance with APA style. This reference page does not count toward the total page requirement.

Review the Critical Thinking grading rubric, found in the Week 5 folder, to see how you will be graded for this assignment.

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: Outline – Business Continuity Plan

Submit a first-draft outline of the Business Continuity Plan. The draft should be 2-3 pages in length and contain sufficient detail to determine if the Portfolio Project submission will fulfill the requirements of the assignment. Students should incorporate instructor's feedback into the Portfolio Project due in Module 8.

Option #2: Outline – Business Impact Analysis

Submit a first-draft outline of the Business Impact Analysis. The draft should be 2-3 pages in length and contain sufficient detail to determine if the Portfolio Project submission will fulfill the requirements of

the assignment. Students should incorporate instructor's feedback into the Portfolio Project due in Module 8.

MODULE 6

Readings

- Chapter 10 in *Management of Information Security*
- Cervone, H. (2017). Disaster recovery planning and business continuity for informaticians. *Digital Library Perspectives, 33*(2), 78-81.

Discussion (25 points)

Critical Thinking (75 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: Incident Response Plan

Develop an Incident Response Plan (IRP) for your employer or a firm you are familiar with. Limit your plan to 4-6 incidents that could critically impact the organization. Use the template from the text. Your plan should be 4-6 pages in length.

Your plan should be organized and well-written in conformity with CSU-Global Guide to Writing & APA.

Review the Critical Thinking grading rubric, found in the Week 6 folder, to see how you will be graded for this assignment.

Option #2: Digital Forensics Program

Your CIO asked you to prepare a report outlining the benefits of implementing a Digital Forensics Program. Your report should be 4-6 pages in length and cover the following items:

- Business value of digital forensics
- Brief description of digital forensics
- Description of digital forensics methodology

Your report should be organized and well-written in conformity with CSU-Global Guide to Writing & APA.

Review the Critical Thinking grading rubric, found in the Week 6 folder, to see how you will be graded for this assignment.

MODULE 7

Readings

- Chapter 11 in *Management of Information Security.*
- Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organizational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society, 19*(1), 161-180.

Discussion (25 points)

MODULE 8

Readings

- Chapter 12 in *Management of Information Security.*
- Keegan, N., Ji, S., Chaudhary, A., Concolato, C., Yu, B., & Jeong, D. (2016). A survey of cloud-based network intrusion detection analysis. *Human-centric Computing and Information Sciences, 6*(1), 1-16.

Discussion (25 points)

Portfolio Project (250 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: Organizational Risk & Security Plan

Scenario

You currently serve as an IT security intern for a military defense contractor called Military Delivery Logistics (MDL) based in Washington, D.C. Because your organization contracts with the U.S. military, the organization is required to perform regular risk and security assessments on all its systems.

Senior management at MDL has decided that the existing risk and security management plan for the organization is out of date and that a new risk management plan needs to be developed to stay in compliance with strict military and Department of Defense (DoD) requirements. Because of the importance of risk management to the organization, senior management is committed to, and supportive of, the project to develop a new plan. You have been assigned to develop this new plan.

The risk and security management plan will consist of a number of different sections. You have been asked to draft the Business Continuity section.

Directions

Draft the Business Continuity section of the Risk & Security plan. Assume that MDL has 5 terabytes (TB) of data that needs to be accessible immediately following any disaster or security incident. Account for the following items as key parts of your plan:

1. Describe how to recover a business operation while efforts are ongoing to restart previous operations.
2. Discuss potential vendor partnerships that need to be in place to ensure a speedy recovery and business continuity.
3. Describe a testing plan to correct any issues with the continuity plan.

Helpful Resources

- ISO/IEC 22399:2007 Guidelines for incident preparedness and operational continuity management.
- ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services.

Discuss and cite at least three credible or scholarly sources other than the assigned readings to support your analysis and positions. You may also cite assigned readings as applicable. The CSU-Global Library is a good place to find scholarly sources. Your paper should be 8-10 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

Option #2: Business Impact Analysis

When organizations embark on a contingency planning exercise, the first step is to conduct a Business Impact Analysis (BIA). You are to conduct a BIA on your organization or an organization you are familiar with. The scope of a BIA can require a significant effort, so keep your scope manageable, possibly only assessing a subset of your company's business processes. However, do not analyze only critical processes. Look for a cross-section of processes based on the criticality to the organization.

Ensure your BIA covers the following components:

1. Determine business processes and recovery criticality
2. Identify resource requirements
3. Identify recovery priorities for system resources
4. Use standard recovery metrics such as RTO, MTD, RPO, and WRT in your evaluation

Discuss and cite at least three credible or scholarly sources other than the assigned readings to support your analysis and positions. You may also cite assigned readings as applicable. The CSU-Global Library is a good place to find scholarly sources. Your paper should be 8-10 pages in length with document and citation formatting per CSU-Global Guide to Writing and APA Requirements.

COURSE POLICIES

Course Grading

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

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.