STUDENT COPY

The following sections contain student copies of the assignments. These must be distributed to students prior to the due dates for the assignments. Online students will have access to these documents in PDF format, which will be available for downloading at any time during the course.

Graded Assignment Requirements

Assignment Requirements documents provided below must be printed and distributed to students for guidance on completing the assignments and submitting them for grading.

Instructors must remind students to retain all handouts and assignment documents issued in every unit, as well as student-prepared documentation and graded deliverables. Some or all these documents will be used repeatedly across different units.

Unit 1 Discussion 1: Public and Private Sector Regulatory Requirements

Learning Objectives and Outcomes

- You will explore the concepts of public and private sector regulatory requirements.

Assignment Requirements

You are provided a table worksheet for your group to populate and provide a rationale of compliance laws with which a public or a private organization may have to comply.

Therefore, before participating in this discussion, read through the various compliance laws carefully and then discuss how the private regulatory requirements differ from the public sector regulatory requirements.

At the end of the discussion, summarize the key points and the other students' perspectives in the form of a completed table.

Required Resources

- Worksheet: Public and Private Sector Regulatory Requirements

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 1

Self-Assessment Checklist

- I have provided the proper justification for comparing the public and private sector regulatory requirements and related them to the compliance laws.
- I have correctly identified the laws that would be applicable to the public or private sector.
- I have provided a clear concise rationale for my selection.

Unit 1 Assignment 1: Compliance Laws

Learning Objectives and Outcomes

- You will apply current compliance laws to an organization selected in the assignment.
- You will learn which compliance laws apply to public organizations.

Assignment Requirements

You are assigned to write an introductory analysis of what compliance laws your organization uses. The large public health care organization that recently hired you wants a completed table to submit to the outside auditors coming for the annual audit. The original table was damaged, and the existing one has been taken from the Chief Information Security Officer's (CISO's) memory. Be sure to research and list the compliance laws that an organization of your type and size should have. An internal auditor will verify your work, so any compliance laws your research discovers may be used or removed from the list by him.

Add additional compliance laws and describe their use within the organization. Make a diagram of the frameworks used for the compliance laws affecting your organization. You can use the table provided in the worksheet to accomplish this task. If you find that the table is missing some compliance laws, please add them.

Use the worksheet to populate the table and to explain what compliance laws you believe should be in your organization based on its type. Remember, this is a good time to check carefully to ensure that the table is complete, and the grammar is perfect. This document with table should be two pages or less. Be sure to use The Chicago Manual of Style and reference your research so your manager may add or refine this report before submission to top management.

You will write a summary of this activity:

1. Identifying the compliance laws that are appropriate for the organization.
2. Giving argument for the identified compliance law.
3. Describing what, if any, governance or international applicability exists.

Required Resources

- Worksheet: Compliance Laws

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space

- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 2

Self-Assessment Checklist

Use the following checklist to support your work on the assignment:

- I have clearly labeled all applicable laws relating to a public health care organization.
- I have properly cited all research.
- I have provided a rationale for my selection.

Unit 2 Discussion 1: Organizational Barriers to Information Technology (IT) Compliance

Learning Objectives and Outcomes

- You will explore the concept of organizational barriers that hinder IT compliance maintenance.

Assignment Requirements

After learning about the organizational barriers in this unit, you are well aware of the fact that there are many barriers to IT compliance.

Taking this information into account, please use the worksheet provided to you for the discussion activity for this unit. In the worksheet, list the various organizational barriers to IT compliance.

Once you have identified the barriers, discuss them in your group. Then, summarize your group's findings in a bulleted format, and provide a rationale for each barrier that your group listed.

Required Resources

- Worksheet: Organizational Barriers to IT Compliance

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 2

Self-Assessment Checklist

- I have provided an adequate list of barriers to the organization.
- I have provided a rationale for each barrier.

Unit 2 Assignment 1: Frameworks—Role in Information Technology (IT) Security Domains and Auditing Compliance

Learning Objectives and Outcomes

- You will be able to identify the role of frameworks in IT security domains and auditing compliance.

Assignment Requirements

You have been designated as the Strategy Development Officer and have been asked to meet the Defense Spectrum Organization (DSO) Director to help him identify the frameworks required to develop the long-term strategies to address the current and future needs for Department of Defense (DoD) spectrum access. This is necessary because the DSO is the center of excellence for electromagnetic spectrum analysis and the development of integrated spectrum plans. It provides direct operational support to the Chairman of the Joint Chiefs of Staff (JCS), Combatant Commanders, Secretaries of Military Departments, and Directors of Defense Agencies to achieve national security and military objectives, and your analysis will be the first step in helping to develop long-term strategies for the organization.

Draft a complete report addressing the following tasks:

1. Identify three frameworks that fit into the organizational scenario.
2. Analyze the scenario based on the identified frameworks.
3. Develop a plan to audit the three identified frameworks for compliance.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 3

Self-Assessment Checklist

- I have identified the three frameworks.
- I have provided an adequate analysis.
- I have designed an appropriate plan for compliance using the correct format.

Unit 3 Discussion 1: Information Gathering

Learning Objectives and Outcomes

- You will learn the various methods to gather information from the organization when preparing to conduct an audit.

Assignment Requirements

In groups, discuss five methods to gather information for an audit, using a typical organization.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 3

Self-Assessment Checklist

- I have created a list of at least five different methods to gather information for an audit.

Unit 3 Assignment 1: Analyzing the Critical Security Control Points

Learning Objectives and Outcomes

- You will be able to analyze the critical security control points in the information technology (IT) infrastructure.

Assignment Requirements

Your organization, the Defense Information Systems Agency (DISA), has many areas of expertise; however, the Defense Spectrum Organization (DSO) Director has asked for your help. The DSO is the center of excellence for the electromagnetic spectrum analysis and the development of integrated spectrum plans and long-term strategies to address current and future needs for the Department of Defense (DoD) spectrum access. DSO provides direct operational support to the Chairman of the Joint Chiefs of Staff (JCS), Combatant Commanders, Secretaries of Military Departments, and Directors of Defense Agencies to achieve national security and military objectives. The organization currently uses various frameworks; your manager has asked you to recommend controls that would resolve the tasks below. Also, use the National Industrial Security Program (NIST) controls for the tasks below. Based on this organizational scenario, you must complete the following tasks:

- Identify the critical security control points that must be verified throughout the IT infrastructure.
- Analyze the scenario without the critical security control points.
- Formulate the plans to help the organization strengthen the security control point's verification.
- Summarize the findings in a report.

Write a complete report that addresses the tasks above. Be sure to use The Chicago Manual of Style and reference your research, so your manager may add or refine this report before submission to top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages

- Due By: Unit 4

Self-Assessment Checklist

- I have identified the critical security controls.
- I have created a report using The Chicago Manual of Style.
- I have constructed the report with an introduction and a summary.

Unit 4 Discussion 1: The Importance of Job Role Separation in Organizations

Learning Objectives and Outcomes

- You will learn how each job role adds security to the organization data and lowers the risk.
- You will create a list of typical job roles and learn why they are separated. You will understand why each job role adds to the security by reducing the risk.

Assignment Requirements

The class will be divided into groups to write a report to share with the class about how separating the job roles can reduce the risk to the organization, and why it can add overall security to the organization.

Create a list of possible job roles in three of the seven domains, and describe what each role will be responsible for and why it will be separated. Create a report summarizing your group's findings, and share it with the class.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 4

Self-Assessment Checklist

- I have created examples of job roles from three of the seven domains.
- I have listed my group's rationale as to why each job role will be separated.

Unit 4 Assignment 1: Information Technology (IT) Security Controls and Countermeasure Gap Analysis

Learning Objectives and Outcomes

- You will create a report listing security controls and gap analysis for the scenario below.

Assignment Requirements

You are appointed as an IT security manager in the XYZ health care organization. This large publically-traded health care organization has 25 sites across the region, with 2,000 staff members and thousands of patients. Sean, your manager, has asked you to analyze the available situation of the corporation and to identify and finalize the method for creating the framework for a security policy. He wants to know how you will approach this endeavor.

Conduct research to find examples of the differences between IT security controls and countermeasure gap analysis, and identify tactical, strategic, risk mitigation, threats, and vulnerability dimensions and gaps associated with compliance recommendations.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style, and cite your references, so your manager may add or refine this report before submission to top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 5

Self-Assessment Checklist

- I have formatted the report using The Chicago Manual of Style.
- I have listed each security control with my rationale.
- I have included a countermeasure gap analysis.

Unit 5 Discussion 1: Separation of Duties, Least Privilege, and Need-to-Know

Learning Objectives and Outcomes

- You will understand why various duties are separated.
- You will gain insight into the reasons that data has a need-to-know factor.
- You will understand the concept of least privilege.

Assignment Requirements

As a group, create a list with headings for the three concepts listed above, and list three examples for each.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 5

Self-Assessment Checklist

- I have provided clear examples for the separation of duties.
- I have used the concept of least privilege.
- I have provided the reasons why data access is based on a need-to-know basis.

Unit 5 Assignment 1: Best Practices for User Domain Compliance

Learning Objectives and Outcomes

- You will create a report listing security controls and gap analysis for the scenario below.

Assignment Requirements

Sean, your manager, just came into your office at 6:00 p.m. on Friday, and wants you to complete some tasks over the weekend. He has just been given numerous tasks in the management meeting which ended a few minutes ago, and he is counting on your help to complete this large assignment. Remember, this is a golden opportunity for you, so it is important you complete this assignment in Unit 5, which is due next week. Your medium-sized health care organization is publicly-traded, and it requires the identification of the User Domain compliance in the organization. To Sean's knowledge, these do not exist. Therefore, you will need to research a generic template, and use that as a starting point in the search for compliance documents. Look for the existing policy templates and examples from organizations of a similar type to your organization. Your organization has personal computers (PCs), laptops, servers, and mainframe user access.

Conduct the research and find examples of the best practices for the User Domain compliance in an organization that is publicly- traded in the health care sector.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style and cite your references, so your manager may add or refine this report before submission to top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 6

Self-Assessment Checklist

- I have written the report using The Chicago Manual of Style.
- I have listed and explained the best practices for the User Domain compliance.
- I have considered User Domain compliance as it relates to the health care industry.

Unit 6 Discussion 1: Vulnerability Management in Workstation and LAN Domains

Learning Objectives and Outcomes

- You will be able to characterize vulnerability management and how it applies to the Workstation and Local Area Network (LAN) Domains.
- You will be able to apply the constructs learned here to organizations.

Assignment Requirements

In your groups, discuss the topic of vulnerability management and how it applies to both the Workstation and LAN Domains. Use a large private organization as an example, and discuss this topic.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 6

Self-Assessment Checklist

- I have applied vulnerability management constructs to both the Workstation and LAN Domains.
- I have summarized the findings in a report to share with the class.
- I have involved my peers in the discussion.

Unit 6 Assignment 1: Best Practices for LAN Domain Compliance

Learning Objectives and Outcomes

- You will learn what best practices exist in the Local Area Network (LAN) Domain.

Assignment Requirements

Sean, your manager, just came into your office at 6:00 p.m. on Friday, and wants you to help complete certain tasks over the weekend. He was just given numerous tasks in the management meeting which ended a few minutes ago, and he is counting on you to help with the completion of the tasks. Remember, this is a golden opportunity for you, so it is important for you to complete the assignment in Unit 6, which is due next week. Your medium-sized health care organization is public, and it requires the identification of the Workstation and LAN Domains Compliance in the organization. To Sean's knowledge, these do not exist. Therefore, you will need to search for a generic template and to use that to begin your tasks in the area of compliance. Look for existing policy templates and/or examples from organizations of similar type to your organization. Your organization has personal computers (PCs), laptops, servers, and mainframe user access.

Compile a list of common compliance laws relating to publicly-traded organizations for Workstation and LAN Domains.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style and reference your research, so your manager may add or refine this report before submission to top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 7

Self-Assessment Checklist

- I have explained the differences between information technology (IT) security controls and countermeasures with a gap analysis.
- I have identified the tactical and strategic risk mitigation and the threat and vulnerability dimensions.

Unit 7 Discussion 1: Vulnerability Management in Local Area Network (LAN)-to-Wide Area Network (WAN) and WAN Domains

Learning Objectives and Outcomes

- Explore the vulnerability management concepts for the LAN-to-WAN and WAN Domains.

Assignment Requirements

You will discuss the following question with your peers:

- Which of the two domains, LAN-to-WAN and WAN, is more at risk in terms of vulnerability?

Substantiate your perspective based on facts and information, and respond to the queries of your peers. Remember to submit a report at the end of the discussion summarizing the following:

- Key points discussed
- Different perspectives covered

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 7

Self-Assessment Checklist

I included the following in the discussion:

- Vulnerability Management
  - **Define policy**: Organizations must start out by determining what state of security they desire for their environment.
  - **Baseline the environment**: Once a policy has been defined, the organization must assess the true status of security in the environment and determine where policy violations are occurring.

- **Prioritize vulnerabilities**: Instances of policy violations are then prioritized using risk and effort-based criteria.
- **Mitigate vulnerabilities**: Ultimately, the root causes of vulnerabilities must be addressed.
- **Maintain and monitor**: Organizations' computing environments are dynamic and evolve over time, as do security policy requirements.

Unit 7 Assignment 1: Best Practices for Local Area Network (LAN)-to-Wide Area Network (WAN) and WAN Domains Compliance

Learning Objectives and Outcomes

- Analyze the compliance policy requirements for the LAN-to-WAN and WAN Domains.
- Evaluate each device within the domains for access controls and compliance requirements.
- Use the best practice template to both the LAN-to-WAN and the WAN Domains.

Assignment Requirements

Sean, your manager, just came into your office at 6:00 p.m. on Friday, and wants you to complete certain tasks over the weekend because he has been given numerous tasks in the management meeting, which ended a few minutes ago. He is depending on you to help by completing some of the tasks for him. Remember, this is a golden opportunity for you, so it is important for you to complete this assignment in Unit 7, which is due next week. Your medium-sized health care organization is publicly traded, and it requires the identification of the LAN-to-WAN and WAN Domains Compliance in the organization. To Sean's knowledge, these do not exist. Therefore, you will need to conduct search to find a generic template to use as a starting point for completing this task. Look for existing policy templates and/or examples from organizations of similar type to your organization. Your organization has personal computers (PCs), laptops, servers, and mainframe user access. You now have a chance to show off your junior auditing skills.

Research examples of best practices for LAN-to-WAN and WAN Domains compliance for a large public organization.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style and reference your research, so your manager may add or refine this report before submission to top management.

Required Resources

- Internet access

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style

- Length: 1–2 pages
- Due By: Unit 8

Self-Assessment Checklist

- I have included the best practices from within the LAN-to-WAN and WAN Domains for compliance.
- I have described best practices that would be beneficial to both domains.
- I have written the report using The Chicago Manual of Style.
- I have provided support for the best practices template selection.

Unit 8 Discussion 1: Virtual Private Network (VPN) Tunneling and Performance

Learning Objectives and Outcomes

- Identify the importance of a Remote Access Domain and VPN tunneling performance within the seven domains.
- Identify the balance required when implementing compliance controls on VPN tunnels speed versus security.

Assignment Requirements

Participate in a discussion with your peers on the following questions:

- What are the benefits of having a VPN in an organization?
- What are the controls that you will need in place on the VPN tunnels that are used to carry data traffic from an external source into the organization by using a secure method such as VPN?
- Would the use of Internet Protocol Security (IPSec) be the single answer? If not, what other methods or protocols could you use?

List some controls and processes to minimize the risks and to aid in the compliance of the Remote Access Domain.

Substantiate your perspective based on facts and information, and respond to the queries of your peers.

Remember to submit a summary report at the end of the discussion summarizing the following:

- Key points discussed
- Different perspectives covered
- Selected methods with rationale

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 8

Self-Assessment Checklist

- I have listed the three basic steps required in the remote access process:
  - Identification
  - Authentication
  - Authorization

- I have explained tunneling. It is used when an application message uses an application protocol to send data to a target tunnel, which is then encapsulated inside another packet, as described below:
  1. Your application sends a message to a remote address by using its application layer protocol.
  2. The target address used by your application directs the message to the tunnel interface. The tunnel interface places each of the packets from the application layer inside another packet using an encapsulating protocol. This encapsulating protocol handles tunnel addressing and encryption issues.
  3. The tunnel-packet interface passes the packets to the layers that handle the wide area network (WAN) interface for physical transfer.
  4. On the receiving end, the packets go from the WAN to the remote tunnel interface where the packets are decrypted and re-assembled into the application layer packets and then passed up to the remote application layer.

- I have included one of the following encapsulating protocols:
  - **Generic Routing Encapsulation (GRE)**—A tunneling protocol developed by Cisco Systems as an encapsulating protocol that can transport a variety of other protocols inside IP tunnels.
  - **Internet Protocol Security (IPSec)**—A protocol suite designed to secure Internet Protocol (IP) traffic using authentication and encryption for each packet.
  - **Layer 2 Forwarding (L2F)**—A tunneling protocol developed by Cisco Systems to establish VPNs over the Internet. L2F does not provide encryption—it relies on other protocols for encryption.
  - **Point-to-Point Tunneling Protocol (PPTP)**—A protocol used to implement VPNs using a control channel over Transmission Control Protocol (TCP) and a GRE tunnel for data. PPTP does not provide encryption.

- **Layer 2 Tunneling Protocol (L2TP)**—A tunneling protocol used to implement a VPN. L2TP is a newer protocol that traces its ancestry to L2F and PPTP. Like its predecessors, L2TP does not provide encryption itself.

- I have explained the process of monitoring VPN tunneling and performance for Remote Access Domains.

Unit 8 Assignment 1: Best Practices for Remote Access Domain Compliance

Learning Objectives and Outcomes

- Include the Remote Access Domain in compliance laws, such as Health Insurance Portability and Accountability Act (HIPPA).
- Identify the various components and devices that require a Remote Access Domain in an organization.

Assignment Requirements

You are a network administrator in charge of implementing security controls to the organizations network. This week you are hiding under your desk with a coworker watching for your boss, while thinking about getting another job. Your boss, Sean, shows up at your cubicle, having come around the other way. He needs you to complete certain tasks over the weekend as he has just been given numerous tasks in the management meeting that ended a few minutes ago. He is counting on you to help him complete the tasks. Remember, this is a golden opportunity for you because it is important to complete this assignment, which is due in next week. Your medium-sized health care organization is publicly traded, and it requires the identification of the Remote Access Domain compliance in the organization. To Sean's knowledge, this does not exist. Therefore, you need to search for a generic template to use as a starting point for this project. Look for existing policy templates and examples from organizations of a similar type to your organization. Your organization has personal computers (PCs), laptops, servers, and mainframe user access. They have remote access, so you will be able to submit your work from home. This will be a great opportunity to impress your peers.

Research examples of the best practices for Remote Access Domain compliance for a public organization and describe the controls used.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style to cite your references, so your manager may add or refine this report before submitting to the top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space

- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 9

Self-Review Checklist

- I have explained the various compliance requirements for the Remote Access Domain.
- I have considered the aspect of HIPPA for this organization.
- I have used the proper academic writing constructs, such as The Chicago Manual of Style.
- I found additional material in the ITT Tech Virtual Library or other source.
- I wrote the report with diagrams of the network solutions I proposed.
- I labeled the diagram and the devices in the diagram properly.

Unit 9 Discussion 1: Maximizing Availability, Integrity, and Confidentiality for System/Application

Learning Objectives and Outcomes

- Identify the various controls used to maximize availability, integrity, and confidentiality (A-I-C) through the use of controls and Business Continuity Planning (BCP)/Disaster Recovery Planning (DRP) planning methods.
- Handle the critical and private data separately by using BCP/DRP planning methods, and make sure these processes in the BCP/DRP planning are included.
- Identify the various devices and controls in the System/Application Domain.

Assignment Requirements

You need to participate in a discussion with your peers to answer the following questions.

- What are the different devices or components used in the System/Application Domain?
- Which are the controls that provide security?

When discussing the plan with your peers, keep in mind the following points:

- Ensure that you include BCP/DRP in the discussion because these two plans help in maximizing A-I-C.
- Demonstrate how to handle the data with encryption requirements in your planning.

Substantiate your perspective based on the facts and information, and respond to the queries of your peers. Remember to submit a summary report at the end of the discussion including the following:

- Key points discussed
- Different perspectives covered

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 9

Self-Assessment Checklist

- I have provided a list of devices such as access controls and database and drive encryption.

Unit 9 Assignment 1: Best Practices for System/Application Domain Compliance

Learning Objectives and Outcomes

- Identify various system/application compliances requirements for organizations.
- Verify research findings for existing compliance templates.

Assignment Requirements

This week you are hiding under your desk thinking about getting another job while a coworker watches for your boss. Sean, your boss, shows up at your cubicle having come around the other way. He needs your help to complete certain tasks over the weekend because he has been given numerous tasks in the management meeting that ended a few minutes ago. He is counting on you to help him complete the tasks. Remember that this is a golden opportunity for you because this assignment is due next week. Your medium-sized health care organization is publicly owned, and it requires the identification of the System/Application Domain compliance in the organization. To Sean's knowledge, this does not exist. Therefore, you will need to search for a generic template and use that as a starting point for your assignment. Look for existing policy templates and examples from other organizations similar to your organization. Your organization has personal computers (PCs), laptops, servers, and mainframe user access. They have remote access, so you will be able to submit your work remotely. Remember that your organization has many databases, some of which fall under Health Insurance Portability and Accountability Act (HIPPA) compliance regulations. As a junior Security Assurance Analyst, this is your time to shine in front of your peers. Search for examples of best practices for System/Application Domain compliance for a medium-sized public health care organization.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 10

Self-Assessment Checklist

- I have researched and found suitable System/Application Domain templates.
- I have provided a report detailing best practices for the System/Application Domain.
- I have selected the proper frameworks or ones that could potentially work.
- I have used The Chicago Manual of Style format.

Unit 10 Discussion 1: Acceptable Use Policy (AUP)

Learning Objectives and Outcomes

- Identify the realities of organizational structure and interworking politics used when deploying an AUP.
- Substantiate that the AUP must be the same for all employees of the organization no matter their position or title by understanding that these policies are for compliance and security for all data.

Assignment Requirements

When examining the AUP within organizations, it often becomes difficult to keep just one policy because owners and senior management often want to have more control over their computing systems and feel they can justify it by their positions.

You must participate in a discussion with your peers to answer the following questions related to the above scenario.

- Do you think that the senior management has more to lose than other employees, such as an accounting clerk, if an attack happens on the system?
- Do you support the statement that the senior management should have a different AUP compared to other employees?
- A part owner in an organization does not want to follow the rules, which are in place to protect the organization. Is his attitude an ethical behavior or not?

Substantiate your perspective based on facts and information and respond to the queries of your peers. Remember to submit a report at the end of the discussion summarizing the following:

- Key points discussed
- Different perspectives covered

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages

- Due By: Unit 10

Self-Assessment Checklist

- I have articulated my position either for or against having different AUPs for different employees.
- I have participated in the discussion in a professional manner even in the case of a disagreement.

Unit 10 Assignment 1: Codes of Conduct for Employees and Information Technology (IT) Auditors

Learning Objectives and Outcomes

- List the various codes of conduct possible that could be developed within an organization.
- Identify codes of conduct from various professional Web sites.

Assignment Requirements

This week you are spending all your time looking for a new job, and yet, it is Friday again, and you know what to expect. Sean, your boss, needs you to complete some tasks over the weekend because he has just been given another large group of tasks in the management meeting, which ended a few minutes ago. He is counting on you to help him again on your time off. Remember, this is a golden opportunity for you, and it is important that you complete the assignment in Unit 10, which needs to be finished next week. His boss asked who has been assisting him on the project, and your name was given. Now, your new office waits, but first, you must do some research and develop a report giving examples for the organizational conduct changes that are about to take place within the corporation. All you have to do now is complete this final report, and you will be a manager, so you can go to that same meeting, and get numerous tasks to take home for the weekend!

Refer to various professional Web sites to identify and list the codes of conduct for employees and IT auditors in your organization.

Write a complete report addressing the tasks above. Be sure to use The Chicago Manual of Style format and to cite your references, so your manager may add or refine this report before submitting to the top management.

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: The Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 11

Self-Assessment Checklist

- I have found numerous examples of codes of conduct from professional Web sites.
- I have written an academic paper.

Project

Project Title

Department of Defense (DoD) Audit

Purpose

The main purpose of this project is to research the assurance methodologies and compliance issues. Using the course as a backdrop, develop assurance methods using the existing frameworks within the seven domains of an information technology (IT) infrastructure.

Learning Objectives and Outcomes

You will be able to develop a rough draft of the seven IT infrastructure domain security assurance compliance requirements for your organization.

Required Source Information and Tools

The following tools and resources will be needed to complete this project:

- Course textbook
- Access to the Internet
  - Federal Information Security Management Act (FISMA): http://iase.disa.mil/fisma/index.html
  - DoD instructions or directives: http://www.dtic.mil/whs/directives/
  - Department of Defense Proposes New Information Security Requirements for Contractors: http://www.hhdataprotection.com/2010/03/articles/information-security/department-of-defense-proposes-new-information-security-requirements-for-contractors/
- Project text sheet

Project Logistics

This project is due in Unit 11 of the course. You will have ten weeks to prepare for this project.

The project will have weekly status reports originated from your team stating the progress and milestones achieved starting in Unit 3. In that status, list your team members. These milestones will be the drafts of the information security systems compliance requirements you will be documenting each week starting in Unit 3. They are defined in the assignments/deliverables. Your team will submit unit milestones to the instructor for review and comment prior to the final document being submitted for a grade. These draft submissions are for instructor monitoring and comments only, and are not graded. Each unit should cover all requirements for each domain as it relates to your organization.

You must submit draft work for monitoring and comments to the instructor on units indicated.

Unit	Task	Type of Submission
3	Team member list and initial team meeting	Draft
6	Research on DoD specific requirements and any problems or questions.	Draft
7	Describe information security systems compliance requirements in the User and Workstation Domains and any problems or questions.	Draft
8	Describe information security systems compliance requirements in the local area network (LAN) and LAN-to-Wide Area Network (WAN) Domains and any problems or questions.	Draft
9	Describe information security systems compliance requirements in the WAN and Remote Access Domains and any problems or questions.	Draft
10	Describe information security systems compliance requirements in the System/Application Domain and any problems or questions.	Draft
11	Final assurance master document covering all compliance requirements for all domains to complete the DoD contract your organization has won.	Deliverable

Deliverables

Scenario

You work for an information technology company that recently has won a large DoD contract. This contract will add another 30% to the revenue of your organization, so it is a high priority, high visibility project, and you will be allowed to make your own budget, project timeline, and toll gate decisions. This course project will require you to form a team of 3–4 fellow students (coworkers) and develop the proper DoD security policies required to meet DoD standards for delivery of the technology services your organization will deliver to the DoD agency, which is the U.S. Air Force Cyber Security Center or AFCSC for short. The policies you create must pass DoD-based requirements. Currently, your organization does not have any DoD contracts and, thus, has no DoD-compliant security policies in place.

Your Firms Computing Environment includes the following:

- 12 servers running Microsoft Server 2008 R2, providing the following:
  - Active Directory (AD)
  - Domain Name System (DNS)
  - Dynamic Host Configuration Protocol (DHCP)

- Enterprise Resource Planning (ERP) Application
- Research and Development (R&D) Engineering
- Microsoft Exchange Server for E-mail
- Symantec e-mail filter
- Websense for Internet use

- 390 plus PCs/laptops running Microsoft Windows 7, Microsoft Office 2007, Adobe, Visio, and Microsoft Project.
- Two Linux servers running your Web site and Cisco routers and Firewalls.

Tasks

You need to follow these steps:

- Create security controls based on auditing frameworks within the seven domains.
- Develop an information assurance (IA) plan.
- List the requirements for each of the seven domains.

Deliverables and format:

Submit your answer in a Microsoft Word document in 2 pages or less.

Font: Arial 10 point size

Line Spacing: Double

Self-Assessment Checklist

- I have used The Chicago Manual of Style format to cite my resources properly.
- I have developed security controls based on the seven domains.
- I have developed a draft IA plan.
- I have included the requirements for each of the seven domains.

Miscellaneous

In your research you will need to use the ITT Tech Virtual Library and other DoD resources to develop your IA controls, so the plan you submit will pass their requirements.

- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction—DoDI 8510.01
  - http://iase.disa.mil/diacap/
  - http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

- Federal Information Security Management Act (FISMA)
  - http://iase.disa.mil/fisma/index.html
- DoD Information Assurance (IA) workforce certification standards DoD Directive 8570.01-M
  - http://iase.disa.mil/policy-guidance/8570_faq_6_12_09.doc
- If you need DoD instructions or directives:
  - http://www.dtic.mil/whs/directives/
- DoD Information Security Program
  - http://www.fas.org/irp/doddir/dod/5200-1r/
- Department of Defense Proposes New Information Security Requirements for Contractors
  - http://www.defense.gov/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html