# STUDENT COPY

Graded Assignments

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: Importance of Security Policies

**Learning Objectives and Outcomes**

* You will be able to learn the importance of information security policies and the role they play in the business activities, ensuring sound and secure information.

Assignment Requirements

Just think about how you would feel if there were no rules regarding how your credit card information was stored on merchants’ Web sites. Would you purchase items from the Web? Would the Internet be as big as it is today if we had no laws or information security policies regarding data that makes up an
e-commerce transaction?

Imagine that you work for an organization that has no Internet use policy so people use the Internet in whatever way they want to by using the company’s personal computers (PCs). Could this cause a problem for the organization?

The answer to these questions is obvious. Security policies are essential in today’s world. However, the flip side to this is that at times these policies also cause problems.

Use the four IT security policies listed below to discuss which are relevant for individuals or for organizations and to what degree these can protect them.

* Internet use policy
* External device use policy
* Employee Identity (ID) policy
* Computer use policy

Also, discuss how these policies actually help or hinder you or your organization.

Respond to your peers and comment on the rationale provided by them for their opinions. Also, summarize your learning in the form of a report enumerating your rationale on the given security policies for both personal use of the Web and your company’s information.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have listed four potential security policies that would satisfy this assignment’s requirement.
* I have listed the rationale for selecting these potential security policies.

## Unit 1 Assignment 1: Security Policies Overcoming Business Challenges

**Learning Objectives and Outcomes**

* You will be able to learn the importance of Information Security Policies and the role they play in business activities to ensure sound, secure information.

Assignment Requirements

Use the same scenario that you used in the Laboratory section of this unit. You have already created an Internet-use policy for the health care organization to protect it against unwanted viruses and various other security breaches. Now use the Lab 1.1 scenario to identify what the possible four information technology (IT) controls would look like by developing an example for each control.

Required Resources

* Unit 1. Lab 1. Alignment of Information Security Policies with Business Objectives

Submission Requirements

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

Self-Assessment Checklist

* I have listed four IT controls based on this unit’s presentation.
* I have provided the required number of IT security controls.
* I have provided a rationale for the IT security controls.

## Unit 2 Discussion 1: Risk Mitigation

**Learning Objectives and Outcomes**

* Using the Nayana Communications case study, provide a risk mitigation strategy to further reduce risk for the organization.

Assignment Requirements

You are provided a case scenario in the lab and homework assignments of this unit. Before you start work on these assignments, you need to discuss among yourselves the need for the development of risk mitigation strategies.

Therefore, before participating in this discussion, read the scenario carefully and discuss how the concept of risk mitigation relates to the scenario. For example, why would the company wish to protect and maintain its high-traffic network? Would it be important to ensure network safety against botnets, keyloggers, worms, or distributed denial of service (DDoS) attacks?

At the end of the discussion, write a summary of your learning from the discussion and submit it to your instructor.

Required Resources

* Access and read the following case study before starting the exercise:
www-935.ibm.com/services/id/gts/pdf/nayana\_communications\_case\_study.pdf (accessed: September 8, 2010)
* Unit 2. Lab 1. Implementation Issues

Submission Requirements

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

Self-Assessment Checklist

* I have identified risk associated with case study and have clearly examined them.
* I have recommended additional risk reduction approaches.

## Unit 2 Assignment 1: Good Policy Implementation

**Learning Objectives and Outcomes**

* You will be able to explore the concept of good policy implementation and describe factors relating to its success.

Assignment Requirements

You will be provided lab handouts. In the lab scenario, two health care organizations have recently merged. However, one is a flat organization and the other is a hierarchical organization. These organizations are in the process of aligning their operations. You are asked to make major refinements to the organization’s cell phone use policy immediately.

Read the scenario carefully and then research examples of good policy implementation.

Write a report citing examples for each of the successful policy implementations found in your research, how you would analyze your organization, and then how you would identify and finalize the method for creating a cell phone use policy for it. In addition, provide a rationale as to what types of business challenges would be overcome or enhanced.

Required Resources

* Unit 2. Lab 1. Implementation Issues

Submission Requirements

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

Self-Assessment Checklist

* I have written an academic paper clearly.
* I have provided an adequate summary.
* I have provided at least three sound policies implementations.

## Unit 3 Discussion 1: Business Considerations

**Learning Objectives and Outcomes**

* You will explore the concepts of business considerations as applied to a scenario.

Assignment Requirements

You are provided a case scenario in the lab and homework assignments of this unit. Before you start to work on these assignments, you need to discuss among yourselves the need for the development of business considerations. Identify business considerations relating to security policy frameworks.

Therefore, before participating in this discussion, read the scenario carefully and discuss why it is important to align the business objectives with the correct framework. Also, discuss what can happen if those frameworks do not fit the business objectives and why is it important to pay attention to business objectives.

At the end of the discussion, list at least four things that could affect the business if the incorrect security framework is used, including the rationale for each. Also, write an example of what could happen if the framework does not align with the business. Finally, write a summary of your findings and submit it to your instructor.

Required Resources

* Unit 3. Lab 1. Inter-relation of Security Policy Frameworks

Submission Requirements

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

Self-Assessment Checklist

* I have responded with answers or suggestions that clearly indicate my understanding of the requirements.

## Unit 3 Assignment 1: Security Policy Frameworks

**Learning Objectives and Outcomes**

* You will learn how some frameworks inter-relate in industry specific organizations.
* You will explore different frameworks and show how they inter-relate.

Assignment Requirements

You work for a governmental organization with Department of Defense (DoD) ties, and as a junior security analyst, you have been asked by your manager to identify and explain three business considerations relating to the security policy frameworks and describe the factors relating to them, especially for a DoD type of organization. Remember that your organization’s long term strategic goal is to make DoD its primary focus of business and in doing so, your organization will be faced with a different set of business considerations, that is, DoD contracts their security level requirements and time constraints.

You need to create a table showing three DoD frameworks and align them to your firm’s business considerations, that is, to be a DoD-focused organization. Write an introduction, including the table created above, describing business considerations relating to a DoD-supplier organization. Be sure to include a conclusion and rationale.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have provided a table with three frameworks that inter-relate.
* I have provided a rationale for selecting the frameworks that would inter-relate.

## Unit 4 Discussion 1: Separation of Duties (SOD)

**Learning Objectives and Outcomes**

* You will learn the reasons why SOD is a critical requirement for policy framework compliance.
* You will also learn how to develop SOD policies.

Assignment Requirements

Participate in a discussion on the importance of the SOD for personnel. Discuss examples of what roles would always be separated. For example, an administrator has server login access, and a user will have system login details. Payroll has access to the records, but it cannot give out raises, only payroll managers can give out raises, etc.

At the end of the discussion, submit a summary of your learning as a bulleted list that explains the importance of the SOD for personnel. For a submission on a discussion task, either respond in class or post some of your findings on the board.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have provided enough content.
* I have provided a methodology for creating a security policy.
* I have provided a reasonable approach to organizational analysis.

## Unit 4 Assignment 1: Security Policy Creation

**Learning Objectives and Outcomes**

* You will research information security policy framework approaches. You will analyze policies for the specified organization.
* You will identify the method for creating a security policy framework.

Assignment Requirements

You are appointed as an information technology (IT) security manager in the XYZ health care organization. This publically traded, large 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 then to identify and finalize the method for creating a security policy framework. He wants to know how you would approach this endeavor. Write a report on how you would analyze your organization and how you would go about identifying and finalizing the method for creating a security policy framework. He will then compare your findings to his and move forward to make the changes that were applicable. Be sure to research these steps from the textbook, ITT Tech Virtual Library, and use these methods to formulate your recommendations. Complete a report no longer than three pages describing how you would approach the task above.

Required Resources

* Textbook: Johnson, Rob, and Merkow. *Security Policies and Implementation Issues.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.
* ITT Tech Virtual Library

Submission Requirements

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

Self-Assessment Checklist

* I have identified the method for creating a security policy framework*.*

## Unit 5 Discussion 1: Best Practices for User Policies

**Learning Objectives and Outcomes**

* You will learn how using a security awareness policy (SAP) can increase the level of security understanding within the organization.
* You will learn the topics to include in the SAP.

Assignment Requirements

You need to discuss among yourselves the various key items that must be included in the SAP. This discussion should incorporate the two most important practices and explain why they are so highly ranked.

At the end of the discussion, you need to list the top two items that must be included in the SAP. Also, provide a rationale for your selection and submit it to your instructor.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have listed the top two items that must be included in the SAP.
* I have provided a rationale for selecting them.

## Unit 5 Assignment 1: Create User Policy

**Learning Objectives and Outcomes**

* You will be able to create a report detailing user access policies based on research.
* You will be able to explain the details of user policy creation in organizations.

Assignment Requirements

You work for a private and medium-sized health care organization that has server, mainframe, and Rivest, Shamir, and Adleman (RSA) user access. Your organization requires identification of the types of user access policies provided to its employees. Sean, your manager, just came into your office at 6:00 p.m. on Friday and asks you to write a report detailing these user access policies. He needs you to research a generic template and use that as a starting point to move forward with. He wants you to complete this task over the weekend as he has just been given a boat load of tasks in the management meeting which ended a few minutes ago. He is counting on you to take some of the load off his shoulders. This is due next week.

Look for existing policy templates and examples from organizations of similar type.

Write a report detailing these user access policies based on your research, and place them into a table with an introduction explaining the following: Who? What? When? Why? Be sure to add a conclusion with a rationale for your selection. 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: Chicago Manual of Style
* Length: 1–2 pages
* Due By: Unit 6

Self-Assessment Checklist

* I have created a table listing policies for the given scenario.
* I have used references.
* I have formulated my report clearly.
* I have provided a rationale and conclusion.

## Unit 6 Discussion 1: IT Infrastructure Security Policies

**Learning Objectives and Outcomes**

* You will learn how different policies affect the information technology (IT) infrastructure.
* You will learn how security policies reduce the overall organizational risk.

Assignment Requirements

Participate in the discussion on the best practices for IT infrastructure security policies.

At the end of the discussion, submit a summary of your learning as bulleted list that explains the best practices for IT infrastructure security policies. For a submission on a discussion task, either respond in class or post on the board some of your findings.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have submitted a summary of the best practices for IT infrastructure security policies.
* I have submitted the summary of my learning as bulleted list.

## Unit 6 Assignment 1: IT Infrastructure Policies

**Learning Objectives and Outcomes**

* You will examine information technology (IT) infrastructure policies.
* You will describe IT infrastructure policies based on the scenario given.

Assignment Requirements

The scenario for this assignment builds upon the scenario in Unit 5 Assignment 1. This time, Sean asks you to examine the IT infrastructure policies of the organization.

Write a report detailing these IT infrastructure policies based on your research, and place them into a table with an introduction explaining the following questions: Who? What? When? Why? Be sure to add a conclusion with a rationale for your selection. Reference your research so your manager may add or refine this report before submission to top management.

Required Resources

* Unit 5 Assignment 1 Scenario

Submission Requirements

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

Self-Assessment Checklist

* I have described what IT infrastructure polices would be used in the given scenario.
* I have created a table and populated it with data that answered the deliverable.

## Unit 7 Discussion 1: Business Impact Analysis (BIA), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP)

**Learning Objectives and Outcomes**

* You will learn approaches on how to plan for impacts that could potentially cause disruptions.
* You will learn to create BIA, BCP, and DRP.

Assignment Requirements

Participate in a discussion on the need of policies for BIA, BCP, and DRP and the importance of a plan with information security as a focal point.

At the end of the discussion, submit a summary of your learning as bulleted list that explains the relevance of these policies. For a submission on a discussion task, either respond in class or post on the board some of your findings.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have provided a list of reasons why policies are a requirement for BCP and DRP.
* I have provided a strong case for policy creation for BIA.
* I have worked as a group.
* I have explained my rationale as to why policies are a requirement for these types of plans.

## Unit 7 Assignment 1: Risk Management in a Business Model

**Learning Objectives and Outcomes**

* You will learn various aspects of how risk management impacts the business model.

Assignment Requirements

You work for a private and medium-sized health care organization that has server, mainframe, and Rivest, Shamir, and Adleman (RSA) user access.

For the third week in a row, Sean just comes into your office at 5:00 p.m. on Friday and needs you to write a report describing some of the risks associated with not having all the security items in place. He needs you to research a generic template and use that as a starting point to move forward with. He wants you to complete this task over the weekend.

You, now realize that your organization does not have much in the way of an information security strategy, and is missing many of what you think are critical components. Your organization is Health Insurance Portability and Accountability Act (HIPAA) compliant and follows other external compliance requirements. However you are unsure on how to go about this task.

Look for existing risk outcomes for examples from organizations of similar type as your organization.

Write a report identifying the risks associated with the current position your organization is in, and how using the information security systems policies your organization can mitigate risk. Include an introduction explaining the following: Who? What? When? Why? Be sure to add a conclusion with a rationale detailing how risks can be mitigated. 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: Chicago Manual of Style
* Length: 1–2 pages
* Due By: Unit 8

Self-Assessment Checklist

* I have created a report listing automated IT security compliance systems.
* I have included the organizational information in the report.
* I have addressed systems that would or could be used in that organization.
* I have created an academic paper.

## Unit 8 Discussion 1: Support Services

**Learning Objectives and Outcomes**

* You will learn what types of support services would be deployed when an incident occurs.
* You will explore support services that would be required when an incident impacts the operational performance of an organization.

Assignment Requirements

Participate in the discussion on the need of support services. Discuss various ways to use support services when an incident occurs.

At the end of the discussion, submit a summary of your learning as bulleted list that explains the relevance of these services. For a submission on a discussion task, either respond in class or post on the board some of your findings.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have created a list of support services that could be used by an organization during or shortly after an incident occurs.

## Unit 8 Assignment 1: Create an Incident Response Policy

**Learning Objectives and Outcomes**

* You will create an incident response policy for a health care organization.
* You will explore policy creation for incident response for a health care organization.

Assignment Requirements

The scenario in this assignment builds upon the scenario in Unit 5 Assignment 1. Imagine that you are hiding in the staff lounge waiting for a coworker so you can sneak out of work and miss your boss. Unfortunately, when you turn back, you see him standing there. This time, he tells you to identify the incident response policies that should be used for the organization. To his knowledge no policy exists, so you will have to research and actually build out a policy for incident response.

Look for existing incident response policies for examples from organizations of similar type to your organization.

Create an initial draft for an incident response policy for your organization. Use an existing template and mold it to fit your organization. Write a report describing an Incident Response Policy. Reference your research so your manager may add or refine this report before submission to top management.

Required Resources

* Internet access
* Unit 5 Assignment 1 Scenario

Submission Requirements

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

Self-Assessment Checklist

* I have created a sound policy for incident response.
* I have considered Health Insurance Portability and Accountability Act (HIPAA) and other health care related compliance requirements.

## Unit 9 Discussion 1: Information Dissemination—How to Educate Employees

**Learning Objectives and Outcomes**

* You will explore and discuss security awareness policy creation, training, and application.
* You will learn how to approach or what approaches are possible regarding a security awareness policy (SAP).

Assignment Requirements

Participate in a discussion on information dissemination—how to educate employees. Identify various SAP implementations and discuss how to educate employees.

At the end of the discussion, submit a summary of their learning as a bulleted list that explains the relevance of educating employees on information dissemination.

For a submission on a discussion task, either respond in class or post on the board some of your findings.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have created a list of at least five items relating to an SAP along with a rationale.

## Unit 9 Assignment 1: Policy Monitoring and Enforcement Strategy

**Learning Objectives and Outcomes**

* You will explore policy creation and enforcement actions.
* You will describe policy monitoring and enforcement strategies.

Assignment Requirements

For this assignment, imagine that you work for a Department of Defense (DoD) organization with direct ties to the U.S. Government, and you are a sole supplier to them for military products. Your organization has three different levels of management and of those levels two different unions exist.

The majority of your staff is in another non-supervisory union and you also have contractors. Your organization had approximately 7,000 workers which are located across the U.S. in 35 locations.

You have developed a modified Internet use policy along with a physical access policy. You must invoke these policies at the earliest as a recent security breach has been identified from flaws in these policies. Identify and describe the legal implications of information systems security (ISS) policy enforcement after these new policies are adapted. Describe a policy monitoring and enforcement strategy for your organization.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have described policy enforcement and monitoring.
* I have written an academic paper.
* I have provided a strategy for accomplishing the enforcement and monitoring.

## Unit 10 Discussion 1: Tracking, Monitoring, and Reporting

**Learning Objectives and Outcomes**

* You will explore various methods for tracking, monitoring, and reporting for organizational compliance.
* You will learn why these systems can reduce the manual methods and thus provide a value add to the compliance process.

Assignment Requirements

Discuss tracking, monitoring, and reporting of various compliance systems. Summarize your thoughts in a Word document and submit it to your instructor. Write the summary of your learning as a bulleted list that explains the relevance of tracking, monitoring, and reporting of compliance systems.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have provided an adequate list of three or more tracking, monitoring, and reporting systems in use today.
* I have used the ITT Tech Virtual Library for reference.

## Unit 10 Assignment 1: Automated Policy Compliance Systems

**Learning Objectives and Outcomes**

* You will research automated information technology (IT) systems and create a report detailing one or two of them.
* You will do research and align a selected automated IT system.

Assignment Requirements

The scenario for this assignment builds upon the scenario in Unit 9 Assignment 1. This time, your manager has asked you to describe what an automated IT security policy compliance system would look like for your organization as management is thinking about this as a possible response to recent security compliance incidents. Write a report describing what the automated IT security policy compliance systems would look like for your organization and submit the report to your instructor.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

* I have written an academic paper.
* I have provided adequate research on an automated IT system for compliance aligned to the organizational situation in the given scenario.

# Project

**Department of Defense (DoD) Ready**

**Purpose**

This course project is intended to assess your ability to identify, design, and organize information technology (IT) security policies.

**Learning Objectives and Outcomes**

You will be able to develop first pass IT security policies for their organization and apply learning constructs from the course.

**Required Source Information and Tools**

You will require the following tools and resources to complete this project:

* Course textbook
* Internet access for research
	+ 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 policies you will be creating each week starting in Unit 3 they are defined in the deliverables. Your team will submit to the instructor unit milestones 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, unless the student teams do not submit their team’s milestones, then a 5% grade reduction will occur from the final document, per milestone missed.

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 |
| 4 | Research on DoD specific requirements, and any problems, or questions. | Draft |
| 5 | U.S. compliance laws now affecting the firm, and any problems, or questions. | Draft |
| 6 | DoD policy 1–5, and any problems, or questions. | Draft |
| 7 | DoD policy 6–9, and any problems, or questions. | Draft |
| 8 | DoD policy 10–15, and any problems, or questions. | Draft |
| 11 | Final policies document master covering all policies required to complete DoD contract your organization has won. | Deliverable |

**Deliverables**

Scenario

You work for a technology company that recently has won a large DoD contract. This contract will add over 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 2–3 fellow students (co-workers) 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 (AFCSC). To do this, you must develop DoD approved policies and standards for all your computing equipment (see list below). The policies you create will pass DoD based requirements. Currently, your organization does not have any DoD contracts and thus has no DoD compliant security policies or controls in place, or many at all as you are a new firm of approximately 390 persons.

Your Firms Computing Environment includes the following:

12 Servers running Microsoft (MS) Server 2008 R2, providing the following: Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), enterprise resource planning (ERP) application (Oracle), research and development (R&D) engineering, Microsoft Exchange Server for e-mail, Symantec e-mail filter, Web sense for Internet use.

390 plus personal computers (PCs)/laptops running Microsoft Windows 7, Microsoft Office 2007, Adobe readers, and professional, Visio 2007, MS Project 2007. Your organization also has two Linux servers running your Web site Apache.

Tasks

You should:

* Create policies that are DoD compliant for all organization computing devices
* Develop a listing of any compliance laws required for DoD contracts
* List controls placed on computing devices listed in project handout
* List standards that would be required for all devices listed by IT domain
* Develop deployment plan for implementation of these polices, standards, and controls
* Develop the project deliverables each unit based on that unit’s content
* List all DoD frameworks that your teams find in the final delivery document
* Hold weekly team meetings with the instructor to be sure your team is proceeding correctly
* Although the project is due in unit 11, it is recommended that you complete it by unit 10 as you have a final exam to take in unit 11.

**Deliverables and format:**

Submit your answer in a Microsoft Word document in not more than two pages.

**Font:** Arial 10 point size

Line Spacing: Double

Self-Assessment Checklist

* I have developed DoD policies and standards for our organization’s computing environment.
* I have involved myself in each of the units and asked questions to the instructor.
* I have found additional references from the original list provided in the project handout.
* I have created an academic paper describing the policies, standards, and controls that would make our organization DoD compliant.
* I have submitted my work per the deliverable timeline to the instructor for monitoring and comment.

**Miscellaneous**

In your research you will need to use the ITT Tech Virtual Library and other DoD resources to develop your policies so the equipment you send will pass their requirements.

* Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction—DoDI 8510.01
	+ <http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>
* If you need DoD instructions or directives:
	+ <http://www.dtic.mil/whs/directives/>
* Department of Defense 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>