

## IT 412: Final Project Guidelines and Rubric

### Overview

There are two components to the final project for this course. The first component is a **risk analysis paper**. The second component is a **risk mitigation plan presentation** to stakeholders that illustrates an organization's regulatory position related to a given scenario. This project is divided into **two milestones**, which will be submitted at various points throughout the course to scaffold learning and ensure quality final submissions. These milestones will be submitted in **Modules Three and Five**. The final product will be submitted in **Module Seven**.

In this assignment, you will demonstrate your mastery of the following course outcomes:

- Evaluate federal, regional, and state cyberlaws and ethics regulations for their impact on organizations' IT and computing policies and operations
- Assess personal and professional ethical violations for the extent to which they impact IT and computing within organizations
- Recommend policies and strategies that align with cyberlaw and ethics guidelines for facilitating compliance and addressing non-adherence
- Utilize cyberlaw and ethics guidelines in creating IT-specific codes of ethics for mitigating stakeholder and organizational risk

### Scenario

ABC Healthcare is a startup company with 50 employees. The company's computer network is shown in Figure 1 below. The healthcare data server contains the company's records, including copies of patient health records with personally identifiable data, patient billing, company financials, and forms.

You have been hired as the IT network security officer, reporting directly to the chief information officer (CIO). Currently, there is a network administrator who has very limited experience and worked as a desktop technician prior to joining ABC. This network administrator helped set up the existing network. In addition, ABC plans to hire a desktop technician and a website developer/programmer who will report directly to the CIO.

There are no policies or guidelines for employees' usage of the computers and network. Network setup was done by various vendors, and all of the programs use default usernames and passwords. Wireless access has been set up for staff using wireless laptops. The same wireless access point also provides clients access to the internet. Some staff members bring in their own computers and connect them to the network. Employees use the work systems for personal web browsing and to check personal email accounts.

As part of network security, management set up a video monitoring system throughout the office. Employees are not notified of any monitoring.

There is a copier/printer in the front office that is used by employees. Currently, all unused copies are left next to the copier for recycling.

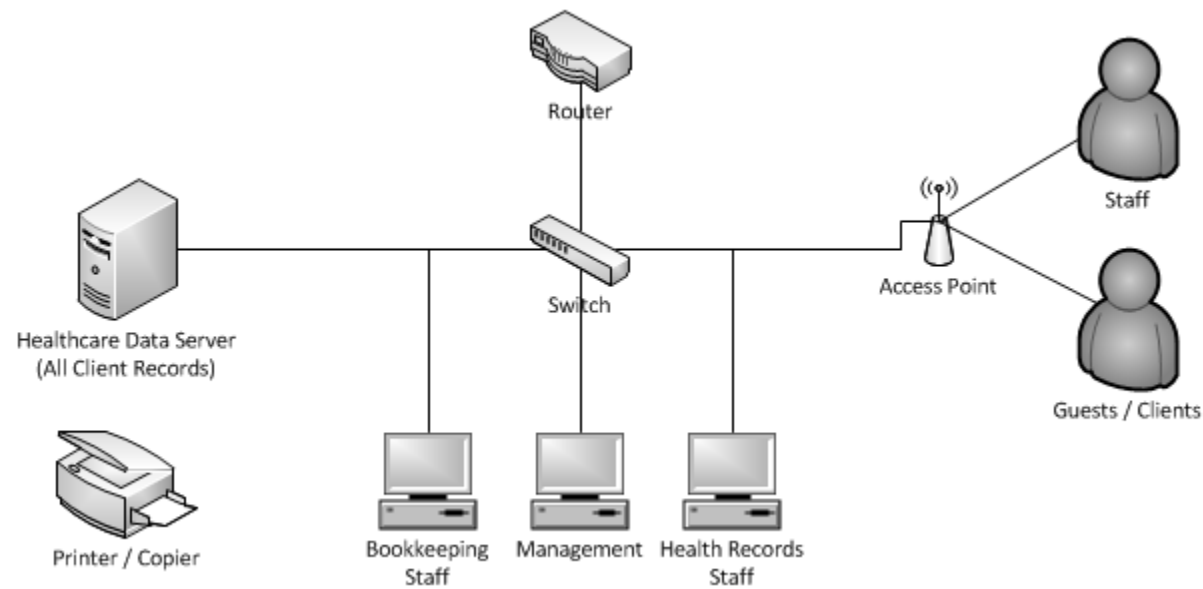


Figure 1

The administration office room uses an open cubicle structure for its staff. Figure 2 depicts the cubicles and seating of its staff. Staff members sometimes complain that they can hear each other during the work day.

Administration Office

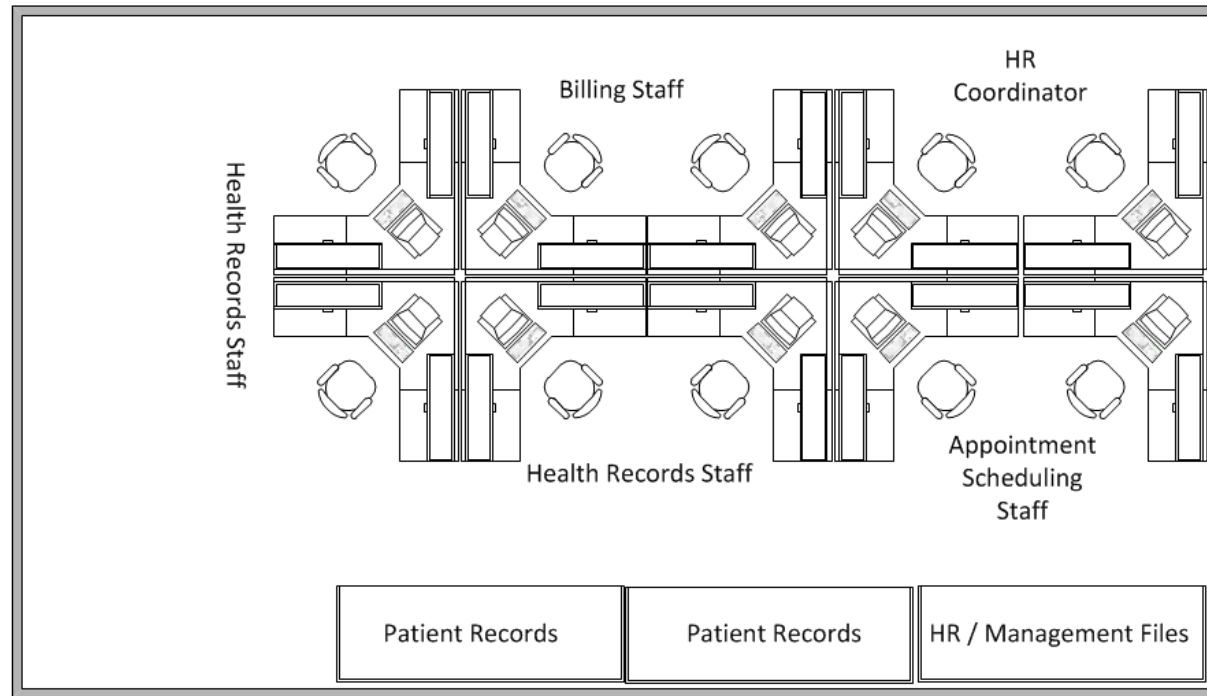


Figure 2

**Prompt**

Create a comprehensive risk analysis narrative in which you assess ABC Healthcare's information systems for ethics violations and cyberlaw compliance, and research the framework for creating an acceptable use-of-technology policy and code of ethics.

Next, using PowerPoint, Google Presentation, or [Prezi](#), create a presentation in which you recommend appropriate strategies for remediating the instances of ethics violations and cyberlaw noncompliance you identified in your risk analysis. Propose an organizational code of ethics related to information technology that prevents future violations and noncompliance, and propose an acceptable use-of-technology policy that addresses non-adherence.

Specifically, the following **critical elements** must be addressed:

I. **Risk Analysis Paper**

1. Describe the **information technology structure** of the organization in the given scenario.
2. Identify specific **cyberlaws and ethics regulations** that pertain to the organization and its computing operations in the scenario.
3. Organizational **ethics violations**
  - i. Classify unethical behaviors with respect to whether they are **personal or professional** in nature, being sure to support your position with specific examples.
  - ii. Assess the **impact** of the unethical behaviors on IT and computing within the organization.
4. **Cyberlaw noncompliance**
  - i. Identify instances of cyberlaw noncompliance, being sure to cite the specific **regulation(s)** being violated.
  - ii. Assess the **impact** of the noncompliance on IT and computing within the organization.
5. **Acceptable use-of-technology policies** research
  - i. **Compare and contrast** acceptable use-of-technology policies from various organizations. You can find suggested organizations below or use policies of your own choosing.
  - ii. Select aspects of the acceptable use-of-technology policies you have researched that you feel could be **adapted** to meet the needs of the organization, and explain how you would adapt them.
6. **Codes of ethics** research
  - i. **Compare and contrast** IT-specific codes of ethics from various organizations. You can find suggested organizations below or use codes of ethics of your own choosing.
  - ii. Select aspects of the codes of ethics you have researched that you feel could be **adapted** to meet the needs of the organization, and explain how you would adapt them.

**IT Acceptable Use Policies**

There are many areas within the field of IT, and each area's policies may vary based on specialization. IT does not have one rule-making body as other professions do. IT does, however, have many professional organizations that represent different specializations, such as security, operations management, and computing technology.

- [SANS Institute Acceptable Use Policy](#)
- [ISSA Acceptable Use Policy](#)
- [Pennsylvania College of Technology IT Acceptable Use Policy](#)
- [AT&T Acceptable Use Policy](#)

### IT Codes of Ethics

Professional organizations provide codes of ethics that may vary slightly, depending on specialization. A code of ethics may also be provided by a business or educational organization.

- [SANS Institute IT Code of Ethics](#)
- [ISSA Code of Ethics](#)
- [K-State Information Technology Employee Code of Ethics](#)

### Business Codes of Ethics

- [AT&T Code of Ethics](#)
- [Microsoft Standards of Business Conduct](#)

- II. **Risk Mitigation Plan Presentation:** Based on your research, you will create a multimedia presentation (suggested length of 5–10 slides) using a tool of your choice (for example, PowerPoint, Google Presentation, or Prezi). Your audience for this presentation is the organization's management. This presentation will provide a brief overview of the issues you identified in your risk analysis and present your recommendations for addressing the problems identified in your analysis. The presentation must include the following **elements**:
- Provide an **overview** of the issues you identified in your risk analysis. In other words, what were the unethical behaviors and instances of cyberlaw noncompliance?
  - Propose appropriate **strategies** that remediate the identified ethics violations and cyberlaw noncompliance. What can the organization do now to address the issues you have identified?
  - Recommend, based on your research, a brief list of appropriate **policy statements** that address acceptable use in facilitating future compliance and addressing non-adherence. In other words, how can the organization prevent the same or similar problem(s) in the future?
  - Recommend, based on your research, a brief IT-specific **code of ethics** that mitigates the risk of future instances of violation and noncompliance. In other words, how can the organization prevent the same or similar problem(s) in the future?

### Guidelines for Presentation:

Your final presentation can be submitted in PowerPoint, Google Presentation, or [Prezi](#) format.

- You can find various template designs on the internet for your presentation. Prior to selecting a specific style, consider your presentation from the perspective of your audience. Avoid distractions. Be consistent with the style of text, bullets, and sub-points to support a powerful presentation that allows your content to be the focus.

- Each slide should include your key point(s). Do not place large blocks of text on the visuals. Add more extensive information in the presenter notes section.
- Use clip art, AutoShapes, pictures, charts, tables, and diagrams to enhance, but not overwhelm, your content.
- Be mindful of your intended audience.

Below are links that offer helpful tips and examples for developing your presentation:

- [Making PowerPoint Slides](#)
- [Beyond Bullet Points: The Better Way to Use PowerPoint](#)
- [Really Bad PowerPoint and How to Avoid It](#)

## Milestones

Milestone One: Draft of Risk Analysis Paper, Sections 1–3

In **Module Three**, you will submit a draft of Section 1: Information Technology Structure, Section 2: Cyberlaws and Ethic Regulations, and Section 3: Ethics Violations. **This milestone will be graded using the Milestone One Rubric.**

Milestone Two: Draft of Risk Analysis Paper, Sections 4–5

In **Module Five**, you will submit a draft of Section 4: Cyberlaw Noncompliance and Section 5: Acceptable Use Policies of the risk analysis paper. **This milestone will be graded using the Milestone Two Rubric.**

Final Submission: Risk Analysis Paper and Risk Mitigation Plan Presentation

In **Module Seven**, you will submit the final risk analysis paper and the risk mitigation plan presentation. These should be complete, polished artifacts containing **all** of the critical elements of the final product. They should reflect the incorporation of feedback gained throughout the course. **This submission will be graded using the Final Project Rubric.**

## Final Project Rubric

**Guidelines for Submission:** Written components of this project must follow these formatting guidelines: double spacing, 12-point Times New Roman font, one-inch margins, and discipline-appropriate citations. The risk analysis paper should be 10–15 pages in length, and the risk mitigation presentation should have 5–10 slides.

**Instructor Feedback:** This activity uses an integrated rubric in Blackboard. Students can view instructor feedback in the Grade Center. For more information, review [these instructions](#).

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
<b>Paper: Information Technology Structure</b>	Meets “Proficient” criteria and uses industry-specific language to establish expertise	Comprehensively describes the information technology structure of the organization in the scenario	Describes the information technology structure of the organization in the scenario, but description is inaccurate or lacks detail	Does not describe the information technology structure of the organization in the scenario	5
<b>Paper: Cyberlaws and Ethics Regulations</b>	Meets “Proficient” criteria and provides specific examples from similar organizations encountered during research	Identifies specific cyberlaws and ethics regulations that pertain to the organization and its computing operations	Identifies specific cyberlaws and ethics regulations but does not connect them to the organization and its computing operations	Does not identify specific cyberlaws and ethics regulations	7
<b>Paper: Ethics Violations: Personal or Professional</b>	Meets “Proficient” criteria, and examination includes harm caused by unethical behaviors	Accurately classifies unethical behaviors as personal or professional in nature and supports position with specific examples	Classifies unethical behaviors inaccurately, or does not support position with specific examples	Does not classify unethical behaviors as personal or professional in nature	7
<b>Paper: Ethics Violations: Impact</b>	Meets “Proficient” criteria and expands on the impact beyond immediate internal stakeholders	Assesses the impact of unethical behaviors on IT and computing within the organization	Assesses the impact of unethical behaviors but does not connect them to the organization, or discussion lacks detail	Does not assess the impact of unethical behaviors on IT and computing within the organization	7
<b>Paper: Cyberlaw Noncompliance: Regulation(s)</b>	Meets “Proficient” criteria, and examination includes harm caused by noncompliance	Accurately identifies instances of cyberlaw noncompliance and cites specific regulation(s) being violated	Identifies instances of cyberlaw noncompliance inaccurately, or does not cite specific regulation(s) being violated	Does not identify instances of cyberlaw noncompliance	7
<b>Paper: Cyberlaw Noncompliance: Impact</b>	Meets “Proficient” criteria and expands on the impact beyond immediate internal stakeholders	Assesses the impact of cyberlaw noncompliance on IT and computing within the organization	Assesses the impact of cyberlaw noncompliance but does not connect it to the organization, or discussion lacks detail	Does not assess the impact of cyberlaw noncompliance on IT and computing within the organization	7

<b>Paper: Acceptable Use Policies: Comparing and Contrasting</b>	Meets “Proficient” criteria, and examples are drawn from a broad range of resources	Comprehensively compares and contrasts acceptable use-of-technology policies	Compares and contrasts acceptable use-of-technology policies, but discussion lacks detail or is inaccurate	Does not compare and contrast acceptable use-of-technology policies	7
<b>Paper: Acceptable Use Policies: Adaptation</b>	Meets “Proficient” criteria and provides detailed examples of how the adaptation will support the organization	Selects aspects of the policies that could be adapted to meet the needs of the organization and explains how they would be adapted	Selects aspects of the policies that could be adapted to meet the needs of the organization, but does not explain how they would be adapted	Does not select aspects of the policies that could be adapted to meet the needs of the organization	7
<b>Paper: Codes of Ethics: Comparing and Contrasting</b>	Meets “Proficient” criteria, and examples are drawn from a broad range of resources	Comprehensively compares and contrasts IT-specific codes of ethics	Compares and contrasts codes of ethics, but codes are not IT-specific, or discussion lacks detail or is inaccurate	Does not compare and contrast IT-specific codes of ethics	7
<b>Paper: Codes of Ethics: Adaptation</b>	Meets “Proficient” criteria and provides detailed examples of how the adaptations will support the organization	Selects aspects of codes of ethics that could be adapted to meet the needs of the organization and explains how they could be adapted	Selects aspects of codes of ethics that could be adapted to meet the needs of the organization, but does not explain how they would be adapted, or explanation is not accurate	Does not select aspects of the codes of ethics that could be adapted to meet the needs of the organization	7
<b>Presentation: Overview</b>	Meets “Proficient” criteria and uses industry-specific language to establish expertise	Provides a comprehensive overview of the issues identified in the risk analysis	Provides an overview of the issues identified in the risk analysis, but the overview lacks detail	Does not provide an overview of the issues identified in the risk analysis	6
<b>Presentation: Strategies</b>	Meets “Proficient” criteria and provides detailed examples of how the proposed strategies will remediate the identified issues	Proposes appropriate strategies that remediate the identified ethics violations and cyberlaw noncompliance	Proposes strategies that remediate the identified ethics violations or cyberlaw noncompliance, but not both, or the proposed strategies are inappropriate	Does not propose appropriate strategies that remediate the identified ethics violations and cyberlaw noncompliance	7
<b>Presentation: Policy Statements</b>	Meets “Proficient” criteria and provides detailed examples of how the proposed policy statements will facilitate noncompliance and address non-adherence	Recommends appropriate policy statements that address acceptable use in facilitating compliance and addressing non-adherence	Recommends policy statements that address acceptable use in facilitating compliance or addressing non-adherence, but not both, or recommended policy statements are inappropriate	Does not recommend policy statements that address acceptable use in facilitating compliance and addressing non-adherence	7



<b>Presentation: Code of Ethics</b>	Meets "Proficient" criteria and provides detailed examples of how the proposed code of ethics will mitigate the risk from the identified issues	Recommends appropriate code of ethics that mitigates the risk of future instances of violation and noncompliance	Recommends code of ethics that mitigates risk of future instances of violation or noncompliance, but not both, or the recommended code of ethics is inappropriate	Does not recommend code of ethics that mitigates risk of future instances of violation and noncompliance	7
<b>Articulation of Response</b>	Submission is free of errors related to citations, grammar, spelling, syntax, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations, grammar, spelling, syntax, or organization	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas	5
<b>Earned Total</b>					<b>100%</b>