IHP4 — IHP4 TASK 1: LEGAL ANALYSIS

LEGAL ISSUES IN INFORMATION SECURITY — C841
PRFA — IHP4

COMPETENCIES

4045.1.1 : Compliance Legal Requirements
The graduate describes the legal requirements to address compliance with cybersecurity policies and procedures with an organization.

4045.1.2 : Protection Against Security Incidents
The graduate analyzes applicable laws and policies to legally protect the organization against security incidents.

INTRODUCTION

This course addresses the laws, regulations, authorities, and directives that inform the development of operational policies, best practices, and training. These standards assure legal compliance and minimize internal and external threats.

In this task, you will analyze legal constraints and liability concerns that threaten information security within the given organization and develop disaster recovery plans to ensure business continuity.

SCENARIO

Review the attached "TechFite Case Study" for information on the company being investigated. You should base your responses on this scenario.

REQUIREMENTS

Your submission must be your original work. No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. The similarity report that is provided when you submit your task can be used as a guide.

You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.

*Tasks may **not** be submitted as cloud links, such as links to Google Docs, Google Slides, OneDrive, etc., unless specified in the task requirements. All other submissions must be file types that are uploaded and submitted as attachments (e.g., .docx, .pdf, .ppt).*

A. Demonstrate your knowledge of application of the law by doing the following:
   1. Explain how the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act *each* specifically relate to the criminal activity described in the case study.
   2. Explain how **three** laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study.
   3. Discuss **two** instances in which duty of due care was lacking.
   4. Describe how the Sarbanes-Oxley Act (SOX) applies to the case study.

B. Discuss legal theories by doing the following:
   1. Explain how evidence in the case study supports claims of alleged criminal activity in TechFite.
      a. Identify who committed the alleged criminal acts and who were the victims.
      b. Explain how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity.
   2. Explain how evidence in the case study supports claims of alleged acts of negligence in TechFite.
      a. Identify who was negligent and who were the victims.
      b. Explain how existing cybersecurity policies and procedures failed to prevent the negligent practices.

C. Prepare a summary (*suggested length of 1–2 paragraphs*) directed to senior management that states the status of TechFite's legal compliance.

D. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

E. Demonstrate professional communication in the content and presentation of your submission.

File Restrictions

File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( )
File size limit: 200 MB
File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, csv, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

RUBRIC

A1:COMPUTER FRAUD AND ABUSE ACT AND ELECTRONIC COMMUNICATIONS PRIVACY ACT

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation of how the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act relate to the criminal activity in the case study is not provided.	The explanation of how the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act *each* relate to the criminal activ-	The explanation of how the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act *each* specifically relate to the

	ity in the case study is unclear or incomplete.	criminal activity in the case study is clear and complete.

A2:EXPLANATION OF LAWS, REGULATIONS, OR LEGAL CASES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation of how the 3 identified laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study is not provided.	The explanation of how the 3 identified laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study is illogical, incomplete, or unclear.	The explanation of how the 3 identified laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study is logical, complete, and clear.

A3:DUTY OF DUE CARE

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A discussion of 2 instances in which duty of due care was lacking is not provided.	The discussion illogically addresses 2 instances in which duty of due care was lacking.	The discussion logically addresses 2 instances in which duty of due care was lacking.

A4:SARBANES-OXLEY ACT (SOX)

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A description of how SOX applies to the case study is not provided.	The description provides inapplicable evidence of how SOX applies to the case study, or the description is unclear.	The description clearly provides applicable evidence of how SOX applies to the case study.

B1:CRIMINAL EVIDENCE

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation that contains logical support from the case study to support claims of alleged criminal activity in TechFite is not provided.	The explanation contains illogical support from the case study to support claims of alleged criminal activity in TechFite.	The explanation contains logical support from the case study to support claims of alleged criminal activity in TechFite

B1A:CRIMINAL ACTS: ACTORS AND VICTIMS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Neither the individuals or groups who committed the alleged criminal acts nor the victims of these acts are identified.	1 or more of the individuals or groups who committed the alleged criminal acts or the victims of these acts are incorrectly identified.	*Both* the individuals or groups who committed the alleged criminal acts and the victims of these acts are correctly identified.

B1B:CRIMINAL ACTS: CAUSES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation of how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity is not provided.	The explanation illogically addresses how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity.	The explanation logically addresses how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity.

B2:NEGLIGENT ACTS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation that contains logical support from the case study to support claims of alleged acts of negligence in TechFite is not provided.	The explanation contains illogical support from the case study to support claims of alleged acts of negligence in TechFite.	The explanation contains logical support from the case study to support claims of alleged acts of negligence in TechFite.

B2A:NEGLIGENCE: ACTORS AND VICTIMS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Individuals or groups who were negligent or the victims of the acts of negligence are not identified.	The individuals or groups who were negligent and the victims of the acts of negligence each are incorrectly identified.	The individuals or groups who were negligent and the victims of the acts of negligence each are correctly identified.

B2B:NEGLIGENCE: FAILED PREVENTION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation of how existing cybersecurity policies and procedures failed to prevent the	The explanation illogically addresses how existing cybersecurity policies and procedures	The explanation logically addresses how existing cybersecurity policies and procedures

negligent practices is not provided.	failed to prevent negligent practices.	failed to prevent negligent practices.

C:LEGAL COMPLIANCE SUMMARY

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A summary directed to senior management that states the status of TechFite's legal compliance is not provided.	The summary directed to senior management that states the status of TechFite's legal compliance is unclear or incomplete.	The summary directed to senior management that states the status of TechFite's legal compliance is clear and complete.

D:SOURCES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not include both in-text citations and a reference list for sources that are quoted, paraphrased, or summarized.	The submission includes in-text citations for sources that are quoted, paraphrased, or summarized and a reference list; however, the citations or reference list is incomplete or inaccurate.	The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available. Or the candidate does not use sources.

E:PROFESSIONAL COMMUNICATION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Content is unstructured, is disjointed, or contains pervasive errors in mechanics, usage, or grammar. Vocabulary or tone is unprofessional or distracts from the topic.	Content is poorly organized, is difficult to follow, or contains errors in mechanics, usage, or grammar that cause confusion. Terminology is misused or ineffective.	Content reflects attention to detail, is organized, and focuses on the main ideas as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.

SUPPORTING DOCUMENTS

TechFite Case Study.docx