**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.** The CFAA was made so that unauthorized access to computer systems and computer related crimes could be avoided. Employees made fake accounts so that they could access information not in their scope of work this very clearly violates the CFAA act. Another act is the ECPA which addresses the interception of online communications and access without authorization to stored data about communications between 2 or more people. If the employees who made fake accounts to access information were found to have read communications this would violate the ECPA which would be very likely.

**2. Explain how three laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study.** (The submission appropriately explains that the GDPR is a regulation that applies in the justification of legal action. The response is insufficient because two more specific laws, regulations, or legal cases that apply in the justification of legal action could not be found.) The CFAA computer fraud and abuse act was broken because techfit did penetration tests and scans on the clients’ network which would be considered as hacking and unauthorized. Another law that was broken was the UTSA United states uniform defend trade secrets act because the NDA was assumed to be broken by techfite. Lastly, the Sarbanes-Oxley Act (SOX) was broken because techfite failed to implement company policies that would have data loss prevention enforced, deletion of accounts from employees that were non longer at the company and the correct privileges in the law of least privilege.

**3. Discuss two instances in which duty of due care was lacking.** One instance of lack of duty care was the lack of supervision of employee actions and potential consequences. This includes the relationship which may have given an unfair raise and advantages to Nadia Johnson or the gaining unauthorized access to data that employees were not allowed to get. Another was the lack of segregation of data. Failure to secure the client's data was another one. We yhad nda’s and we did not keep the data safe from unauthorized users.

**4. Describe how the Sarbanes-Oxley Act (SOX) applies to the case study.** One part of the Sox is whistleblower protection, a whistleblower is someone who speaks up about an issue in the company to the SEC. If there was protection employees could speak up about the things that happened at Techfite. Another aspect of SOX was internal reports and reporting requirements, the creation of fake companies to move money and irregularities in the company would break this.

**B. Discuss legal theories by doing the following:**

**1. Explain how evidence in the case study supports claims of alleged criminal activity in TechFite.** There is a lot of evidence in the case study that shows criminal activity. One such piece of evidence is the failure to protect customer data. This would violate data protection laws such as the GDPR in Europe or the GLBA privacy act ECPA or any law of that sort. The relationship between Nadia Johnson and Karl Jaspers would indicate potential bribery or corruption in the company. Finally the evidence that Techfite has dummy companies to move money around would indicate fraud or money laundering.

**a. Identify who committed the alleged criminal acts and who were the victims. ()**The applications department who was led by Karl Jaspers had multiple data breaches of NDAs and mishandled secrets of trade and had financial fraud behaviors. Carl Jaspers was connected to dummy companies and also had a suspicious relationship with Nadia Johnson who received very questionable treatments such as multiple raises. Other employees such as Sarah Miller, Megan Rogers, and Jack Hudson, took part in the unauthorized scanning of other companies’ networks and potentially other illicit activities which could be labeled as penetration testing or hacking. The victims were the clients that did business with TechFit and also the competing companies. Other tragic victims were Techfite itself and its shareholders. Techfite could have reputational damage, loss of capital and stock value which would affect shareholders

**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.** While there were security measures against external threats such as penetration testing there was little to protect the company internally more specifically in the BI department and the applications department.

**a. Identify who was negligent and who were the victims.**(The submission appropriately identifies the BI Unit as negligent. The response is insufficient because at least one more negligent party is not identified.)The negligent people and groups were the BI Unit, IT unit and the upper management. The BI unit had employees that did dumpster diving and trash surveillance and penetration testing without permission. They should be educated on the laws and know the consequences. The IT department also did not give people the right privileges and did not find out that there were dummy accounts and unauthorized scanning of clients networks. The victims were the shareholders, the company itself and the clients. The clients because they did not get a good service and got their data leaked and the others because the company’s reputation got damaged.

**b. Explain how existing cybersecurity policies and procedures failed to prevent negligent practices.** The audits did not detect suspicious behavior and they were very superficial and not detailed. There was no policy that prevented relationships between people in the company. There was also lack of separation of duties and lack of principle of least privilege in the company.

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

Following a thorough examination of TechFite's Applications Division procedures, it was found that the division's current operating procedures present serious issues with respect to legal compliance. Notably, as demonstrated by the cases involving Orange Leaf Software LLC and Union City Electronic Ventures, the division may have violated non-disclosure agreements (NDAs) by handling private and sensitive information from prospective clients. Given that competitors of these prospective clients have reportedly obtained information comparable to this, abusing confidential information could result in legal ramifications. In addition, the finding that fictitious companies may have been involved in questionable financial transactions raises the possibility of financial irregularities that might breach state and federal regulations controlling financial reporting and business behavior.

Furthermore, the lack of internal cybersecurity procedures, especially in the Business Intelligence (BI) Unit, demonstrates a disrespect for ethical standards and may violate legal protections against illegal access and data breaches. Client confidentiality and data security are seriously threatened by the lack of appropriate safeguards to separate client data, uphold the principle of least privilege, and stop illegal access to critical internal departments (such as legal, HR, and finance). In addition to going against industry best practices, this can also be against the legislation and rules governing data protection. In conclusion, TechFite's present legal compliance status for its Applications Division operations is questionable, requiring prompt and comprehensive corrective action to address these violations and avert possible legal repercussions.