

# A Risk Assessment of Information Security in a Diet Centre Business: A Case Study

Tasneem Annahdi<sup>1</sup>, Duaa Alkubaisy<sup>1</sup> and Luca Piras<sup>2</sup>

<sup>1</sup>College of Computer Science & Information Technology, Imam Abdulrahman Bin Faisal University,  
Dammam, Saudi Arabia

<sup>2</sup>Department of Computer Science, Middlesex University, Hendon Town Hall Building,

{2250500216, daalkubaisy}@iau.edu.sa, L.Piras@mdx.ac.uk


**Keywords:** Risk Assessment, OCTAVE-Allegro Framework, Small and Medium-Sized Businesses, Information Security, Human Error, Vulnerability Assessment, Risk Mitigation.


**Abstract:** This paper employed the framework of Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE-Allegro) to analyse the key risks and challenges faced by the business of Diet Centre X, particularly in terms of security, operational efficiency, and customer trust. The primary concerns identified include data input errors, outdated billing systems, weak password management practices, and a lack of comprehensive security awareness training. These issues pose significant risks to the centre's productivity, financial health, and reputation. Contributions of this paper include the proposal of several lessons learned and solutions: creating a customer registration system that is connected to the client data validation in the management system, along with implementing a validation for all input fields to reduce human errors and upgrading the billing system to remove outdated payment methods and enhance the user interface, and conducting quarterly security awareness training for all employees to increase their preparedness against potential security threats.


## 1 INTRODUCTION

Information security protects information assets in confidentiality, integrity, and availability (C.I.A.) (Samonas and Coss, 2014). Continuous monitoring and updates are necessary for an organization's continuity of data protection. Organizations should implement security in the system development methodology. This implementation will protect sensitive data and mitigate cybersecurity threats, and it will help identify the risks before they become critical issues. Furthermore, each organization has three communities in information security that share values and objectives: general management, IT management, and information security management (Herath et al., 2023). Ultimately, they share the goal of collaborating to protect critical data and systems from threats and implement appropriate countermeasures for identifying and mitigating risks. Organization depends heavily on IT-based systems for

its sustainability (Chairopoulou, 2024). Information security, and risk management techniques (Landoll, 2021), part of the basis for business decision-making, these decisions are made based on trade-offs between the costs of applying information system controls and the benefits of using secured available systems (Pearlson et al., 2024). The organization must first identify and comprehend its risks, especially the risk to its information assets, and then the risk must be measured, evaluated, and assessed (Hubbard, 2020). The primary question revolves around whether the danger a business confronts is more than what it can tolerate. Otherwise, the organization will deem the risk management process satisfactory. If not, the company must take action to bring the risk down to a manageable level (Hillson, 2019). Small and medium-sized businesses nowadays are the target for attackers due to their high-security vulnerabilities and lack of security awareness (Miklian and Hoelscher, 2022). Articles have expressed the importance of cybersecurity awareness, employee training, and risk mitigation (Ugbebor et al., 2024). For small and medium-sized businesses, the consequences of

<sup>a</sup> <https://orcid.org/0009-0004-3504-6524>

<sup>b</sup> <https://orcid.org/0000-0001-5920-7856>

<sup>c</sup> <https://orcid.org/0000-0002-7530-4119>

attacks are devastating to recover from. (Jhanjhi and Shah, 2024) In today's landscape, maintaining small and medium-sized businesses from various threats is crucial for ensuring a secure environment. This paper presents a targeted risk assessment for diet centres, focusing on its broader applicability by keeping the company's identity confidential, referred to as Diet Centre X. Hence, Diet Centre X is committed to empowering individuals to live healthier lives through tailored meal plan subscriptions and expert dietitian consultations. By continually monitoring health assessments, the centre tracks customer progress and provides essential resources, enabling clients to confidently pursue their long-term wellness goals. Diet Centre X does not have a technical team of experts because it is not very useful in its field of business. Still, this decision has negatively impacted the business' information security. Most employees lack security knowledge, and this is very dangerous because, in their day-to-day tasks, they deal with critical business information. Because the managers lack technical knowledge, they have ranked the security measure as the least priority. Given that the most suitable framework approach for Diet Centre X is Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE-Allegro) (Hom et al., 2020a) because it delivers an in-depth risk assessment that matches the operational requirements of the diet centre.

The rest of the paper is organized as follows. In section 2, we discuss the related works of literature on past risk assessment approaches. In section 3, we present an in-depth discussion of the tools and techniques, in section 4 we assess and identify the risks by using the OCTAVE Allegro framework, in section 5 we present the lessons learned, solutions, and recommendations in response to the risks and threats identified, lastly in section 6 we conclude the paper and summarize the findings.

## 2 REVIEW OF RELATED LITERATURE

This section reviews past approaches to information security risk management and the framework tools used in the risk assessment approach, particularly in small and medium-sized businesses like Diet Centre X. This section aims to find the best framework tool to conduct it on Diet Centre X for a risk assessment. In the insurance sector, researchers used two framework tools, the ISO/IEC 27005:2018 (Fahrurozi et al., 2020) and NIST Special Publication 800-30 series (Van Devender, 2023) to

enable organizations to conduct an exhaustive risk assessment. ISO 27005:2018's strengths include offering structured guidelines for identifying and assessing vulnerabilities and all potential threats and providing consistency in monitoring the risks. Their methodology handles large volumes of sensitive customer data, such as personal, financial, and health information. The conducted approach helps insurance companies identify and assess data security, privacy, and regulatory compliance risks and implement targeted risk mitigation strategies for improving data protection and security practices. This approach has enhanced risk management and ensures better alignment with global standards, improving insurance companies' security posture and compliance. (Putra and Soewito, 2023) The researchers showed in their study how organizations with limited funding and basic technological understanding. OCTAVE Allegro focuses on identifying and safeguarding vital information assets, evaluating current security measures, and assessing possible threats and vulnerabilities (Suroso and Fakhrozi, 2018) in addition, it is distinguished by its outstanding features and unparalleled capabilities, making it an undeniable leader in its field due to its methodology's user-friendly nature, which allows organizations with low cybersecurity resources to adapt it. This methodology thoroughly identifies the important assets and vulnerabilities, evaluates risks, and then ranks the risks based on impacts. The OCTAVE Allegro framework will help the organization implement the proper security measures to protect private information and increase awareness. (Hom et al., 2020b) Another small and medium-sized business, a medical clinic has implemented three frameworks, HIPAA (Moore and Frye, 2019), NIST, and ISO/IEC 2700, which have provided the clinic with a thorough approach to an information security risk assessment and a guarantee that the clinic's security procedures are strong, legal, and efficient in all facets of data privacy and cybersecurity. The researchers combined three different frameworks to provide extensive coverage. Each framework provided a distinct advantage, with the NIST framework focusing on the technical angle of cybersecurity risk management and protection procedures. In contrast, HIPAA focuses on the legal angle, addressing certain legal compliance requirements in the healthcare industry. ISO/IEC 27001 focuses on the organizational angle, guaranteeing a comprehensive information security management system. As a result, the researchers got a comprehensive risk management procedure that addresses information security's technological,

managerial, and legal facets. This case study proves that the small healthcare clinic can satisfy legal requirements along with building a strong security infrastructure to protect patient data, lower risks, and monitor its information security policies by integrating the three frameworks HIPAA, NIST, and ISO/IEC 2700, where one framework enhances the others, creating a more robust and compliant system for handling medical data. (Ozeer and Pouye, 2021)

### 3 IN-DEPTH DISCUSSION OF TOOLS AND TECHNOLOGIES

Every small and medium-sized business employs a different framework for its risk assessment based on its operations and the amount of risk it faces. Therefore, using the same framework will not guarantee the same results. This section aims to justify the best framework tool chosen for a risk assessment on Diet Centre X. The framework COSO ERM would have been a good choice since it can be tailored to different industries, along with its strategic risk alignment where it makes sure the organization's objectives are aligned with the risk management; due to that it will provide a holistic risk assessment of the organization; but to meet these goals it will require longer time comparing to OCTAVE Allegro, as a holistic risk assessment will also require a lot of special resources such as experienced employees, and that does not fit with Diet Centre X, where it has unexperienced employees and would want the risk assessment to be focused on a specific aspects of the diet centre. As for NIST RMF and COBIT, they could have been suitable for its clear and structured approach, but its main objective is the IT infrastructure and that does not fit with the diet centre industry where it is not a technical-based company. ISO31000 is known for its flexibility to be tailored to different industries and different risk scenarios, and it does not mainly focus on the IT infrastructure like in NIST RMF and COBIT, but it does not offer clear action outcomes such as with OCTAVE Allegro. Lastly, ISO 27005:2018 and NIST SP 800-30 are good approaches that are known for their clear structures and outcomes in identifying the risks and managing them, but it does only focus on the technical part of information security and do not focus on the operational part such as OCTAVE Allegro, and that's why it could not be suitable to be implemented on the Diet Centre X. These frameworks could be suitable for a diet centre if we were approaching two types of risk assessment frameworks to have a broader comprehensive overview, although in this

paper we will only implement one risk assessment framework. Therefore, OCTAVE Allegro would be the suitable approach to be conducted on Diet Centre X as it provides a clear infrastructure and focuses on the technical and operational aspects of the diet centre such as food safety, customer satisfaction, employee training, and adherence to health standards. Also, it would be more effective to use frameworks that provide operational risk management techniques, this will give a more customized, economic data protection and privacy compliance solution. As this approach provides a comprehensive risk assessment, it is time consuming, especially with the limited staff of Diet Centre X, because each step of the methodology requires employees to follow in detail to achieve a thorough evaluation. Also, it is not guaranteed to delve deeply, like NIST, into the technical aspects of IT security. On the other hand, OCTAVE Allegro focuses on identifying critical assets, assessing operational threats, and providing risk mitigation strategies aligned with the organization's overall mission. In the end, every framework has its strengths and weaknesses, and when comparing OCTAVE Allegro's weaknesses to its strengths when implementing it on Diet Centre X, the weaknesses seem tolerable. OCTAVE Allegro would be more effective for Diet Centre X, as their security requirements are usually far less demanding.

#### 3.1 Diet Centre X

As we intend to make this paper more applicable to any diet center, and not shed light on one company, therefore in this paper, we have kept the name of the company anonymous, and the company name will be referred to as Diet centre X. Diet Centre X is a centre that provides a diet clinic and meal subscription plans. The diet clinic allows customers to book an appointment with a dietitian for a consultation. The consultation session will start with the dietitians, gathering information about the customer's medical history and lifestyle. Secondly, the dietitians will assess the customer by taking the body mass index (BMI). Thirdly, based on the assessment, the dietitian will help the customer set specific health goals and guide the customer through a step-by-step process to achieving that goal. Fourthly, the dietitian will suggest one of the meal subscriptions that Diet Centre X offers. Fifthly, the customer continues the with the front desk customer service employee. They will provide the customer with the meals menu where they can choose a meal for each day of the month based on a menu given. Sixthly, the customer chooses a pickup or home/office delivery. Lastly, the customer

is provided with payment options: credit card, cash, and online payment.

### 3.2 OCTAVE Allegro

The best risk assessment approach for identifying, evaluating, and mitigating the threats and vulnerabilities related to information security in Diet Centre X is Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE-Allegro). This approach starts by identifying operationally critical threats. The approach will identify all possible threats and information processes within Diet Centre X to evaluate security concerns qualitatively. Then, a vulnerability assessment will continue to gauge the degree of danger. The final step is to make suggestions and mitigation solutions available. There should also be ongoing monitoring to ensure better outcomes for the diet centre. These studies anticipate assessing risk analysts and security managers from various organizations in conducting practical and reasonably priced information system risk management for multiple industries. As illustrated in Figure 1, the risk assessment will establish the risk measurement criteria according to Diet Centre X. The second step is developing the information asset profile for critical information. The third step is identifying the information asset containers; the asset container is where the information assets are stored, transported, and processed. The fourth step is identifying the area of concern, and the fifth is identifying the threat scenarios. The first step identifies risks, the second step analyses risks, and the eighth step selects a mitigation approach. Implementing these risk assessment steps at Diet Centre X will guarantee threat identifications and vulnerabilities and propose a mitigation approach to reduce risks.

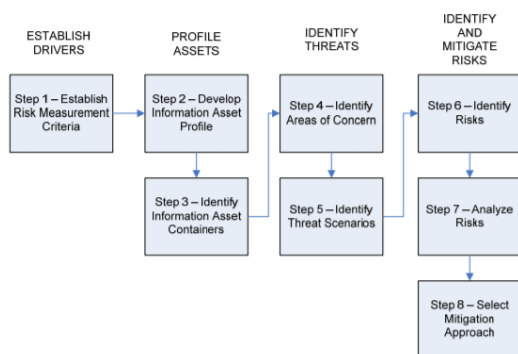


Figure 1: OCTAVE Allegro Roadmap (Suroso and Fakhrozi, 2018).

## 4 RISK ASSESSMENT AND IDENTIFICATION OF RISKS

In this section, we assessed and identified the risks by following the OCTAVE Allegro Road map. We presented details in each of the following steps. In the first section we established the risk measurement criteria, then we developed the information asset profile, afterwards we identified the information assets containers, then we identified the areas of concern, next we identified the threat scenarios, following we identified the risks, ensuing we analysed the risks that were identified, finally we selected the mitigation approach suitable for each identified risk.

### 4.1 Step 1: Establish Risk Measurement Criteria

We started by determining the risk measurement criteria by handing surveys to the IT staff of Diet Centre X. Then, we continued with an interview with each employee. The results of both the surveys and interviews will help us determine the impact area so we can set impact priorities. We also took into consideration Diet Centre X's business objectives and mission. Therefore, the determined impact areas are reputation and customer confidence, finance, productivity, fines and penalties, and safety and health. Based on all the aspects determined, the highest priority of Diet Centre X is reputation and customer confidence, as illustrated in the following figure.

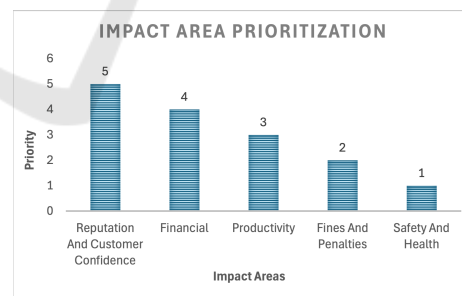


Figure 2: Impact areas prioritization.

Diet Centre X's most crucial business objective is to protect and maintain its reputation and customer confidence for the longest time. Diet Centre X has no limitations on the customer's engagement with the business. There is no particular expiration date for the customers' engagement with the centre. The business depends on always having this customer's financial input. And Diet Centre X's philosophy is that loyal customers attract new customers. Small and medium-sized businesses, such as Diet Centre X, have



been attempting to attract and maintain customers by engaging with customers on a personal level, which is one of Diet Centre X's objectives, and that is what distinguishes Diet Centre X from other businesses in the same field.

## 4.2 Step 2: Develop an Information Asset Profile

In this step, we selected the critical information assets based on the following core process of the diet centre: Customers Assessments and Follow-ups, Food selections, Subscription Services, Billing, Marketing, Staff Training, Customer Service and Support, Technology Management. After outlining the core process procedures, the most important considerations when selecting the critical information assets became more evident. These include whether the asset is essential to the day-to-day business operations, or if the asset is compromised it could disrupt key business functions, after taking these into consideration, we classified the critical assets as: Employee profile, Customer profile, Subscriptions, Customer health info, Customer meal selections and payment details. The following table presents the information asset profile of the customer profile. The table provides vital information about its description, ownership, security requirements, and the most crucial security features.

Table 1: Information Asset Profile of Customer Profile.

<b>Critical Asset</b>	Customer Profile
<b>Rationale for Selection</b>	Customers are the core and most important role of the business processes of the diet centre. The customer profile is used daily in the business.
<b>Description</b>	The asset consists of the customer's personal information, such as name, age, address, gender, health info, phone number, and address.
<b>Owner</b>	IT Division
<b>Security Requirement</b>	<b>Confidentiality:</b> Customer profiles are only accessible by authorized employees. To protect the customers' information from unauthorized users.
	<b>Integrity:</b> The customers' information must be protected from alteration by unauthorized users.
	<b>Availability:</b> Information must be available to customer service employees, dietitians, and customers when needed.
<b>Most Important Security Requirement</b>	<b>Integrity:</b> It is the most important security requirement because if unauthorized users alter the information, it will affect the day-to-day operation, such as the address of the meal delivery or age and gender are critical aspects for the dietitian to set the diet plan.

## 4.3 Step 3: Identify Information Asset Containers

An information asset container is a container for storing, transmitting, and processing information assets. We classified the containers as follows: Technical asset containers are client management systems, cloud storage, and billing systems. Third-party providers are what the employees use to store and process customer information; cloud services such as Google Drive, where the company has a questionnaire for customers' review, Google calendar for scheduling appointments, and Microsoft Forms for the customers' registration forum. Also, communication channels, which are what employees use for communicating with each other or with customers, such as email systems, Instagram, WhatsApp. The following tables outline each information asset container's associated internal and external containers and their owners across tables of technical systems, communication channels, and third-party providers.

Table 2: Information Asset Containers.

Information Asset Risk Environment Map (Technical)	
Internal Container Description	Owner(s)
Client management systems, cloud storage, and billing systems.	IT department, customer service, financial department.

Table 3: Information Asset Containers (Communication Channels).

Information Asset Risk Environment Map (Communication Channels)	
Internal Container Description	Owner(s)
Internal communication channels used for employees' communications are emails and Microsoft Teams.	IT department, HR department.
External Container Description	Owner(s)
External communication channels for customers include emails, Instagram, and WhatsApp.	Customer service, marketing department.

Table 4: Information Asset Containers (Third-Party Providers).

Information Asset Risk Environment Map (Third-Party Providers)	
External Container Description	Owner(s)
Google Drive for customer questionnaires, Google Calendar for appointments, and Microsoft Forms for the customers' registration.	IT department, customer service, and marketing department.

## 4.4 Step 4: Identify Areas of Concern

The areas of concern have been identified based on the significant business challenges where Diet Centre

X must act regarding those concerns, or it will cause tremendous consequences for the business. While monitoring the business's day-to-day operations, we have encountered the following major concerns:

Table 5: Areas of Concern.

No.	Areas of Concern
1	Errors in data input by customer service employees. Due to many customers.
2	Bug/error found in client management systems when the financial staff performs monthly billing reconciliation.
3	A possibility of vulnerability attack by internal/external client management systems.
4	Data leak, theft, or alteration using a third-party provider.

#### 4.5 Step 5: Identify Threat Scenarios

For each area of concern, we detailed their threat scenarios in the following tables to identify the nature of the threat based on the Information Asset Risk Worksheet. In the following tables, the areas of concern numbers correspond to Table 5: Areas of Concern.

Table 6: Threat Scenarios - Area of Concern 1.

Area of Concern	Errors in data input by customer service employees. Due to many customers.
Actor	Customer service employee.
Means	Employees type in data incorrectly.
Motives	By mistake.
Outcome	Disrupt production; whenever an employee needs to retrieve a customer's data, it takes a long time.
Security Requirements	Add validations for each field.

Table 7: Threat Scenarios - Area of Concern 2.

Area of Concern	Bug/error found in client management systems when the financial staff performs monthly billing reconciliation.
Actor	Customer service.
Means	During rush hour, customer service employees may rush and accidentally select the wrong payment type.
Motives	By mistake.
Outcome	When the finance team notices a shortfall in one payment type and a rise in another, it's essential to investigate the causes promptly to maintain financial integrity.
Security Requirements	Add a confirmation popup and improve the interface for better user-friendliness to prevent incorrect button clicks.

Table 8: Threat Scenarios - Area of Concern 3.

Area of Concern	Possible vulnerability attack by internal/external client management systems.
Actor	Attackers.
Means	Harm the company.
Motives	Hack the system.
Outcome	Disrupt production, leak of information, loss of customer trust.
Security Requirements	Monitor periodically the system security to detect loopholes.

Table 9: Threat Scenarios - Area of Concern 4.

Area of Concern	Data leak, theft, or alteration using a third-party provider.
Actor	Inside or outside party.
Means	When using third-party providers, employees share one account with an easily guessed password, which is not regularly updated when employees leave the company; this could make the account vulnerable to outside/inside hacks.
Motives	Harm the business reputation.
Outcome	Disrupt production, leak of information, loss of customer trust.
Security Requirements	Separate account for each employee, with a strong password that is updated periodically.

#### 4.6 Step 6: Identify Risks

By accomplishing the following activities, evaluate how the recorded threat scenarios will impact on the organization: Measure the impact on Diet Centre X in the events that the threat scenarios were to occur. Correspondingly, detail the consequences while taking into consideration the identified impact areas.

#### 4.7 Step 7: Analyse Risks

In this step, we determined the consequences for each area of concern and set the impact value on the organization to high, medium, or low. Then, we calculated the impact area score by multiplying the impact area rank by the impact value. That will help Diet Centre X to develop risk mitigation and control measures. Table 10 illustrates the score calculation.

Table 10: Impact Area Score Calculation.

Impact Areas	Priority	Low	Medium	High
Reputation And Customer Confidence	5	5	10	15
Financial	4	4	8	12
Productivity	3	3	6	9
Fines And Penalties	2	2	4	6
Safety And Health	1	1	2	3

Sometimes customer service employees input error data to the system. So, when retrieving customers' data, they encounter errors; and the chances are low that they will remember the correct input that was supposed to be entered. When, for example, the error was in the client's phone number, this is a massive problem as the centre will not be able to contact the customer, and the customer will be expecting meal delivery from the centre; therefore, the centre will not be able to deliver because the centre will not be able to reach the customer, this will damage the centre's reputation and customer might cancel the subscription and therefore will affect the centre's financial, as illustrated in Figure 3.

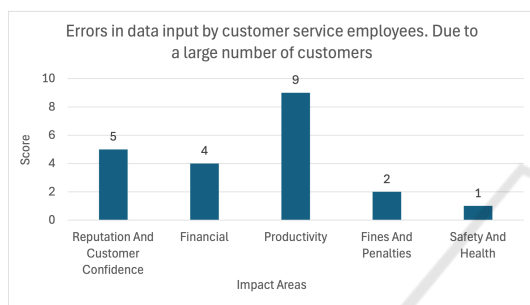


Figure 3: Risk Analysis - Area of Concern 1.

While the customer rushes the customer service employees, they tend to make the mistake of clicking the incorrect payment type. Since the buttons are close to each other and in a small font, employees tend to fall into that mistake, which will later obstruct productivity; where at the end of the month, the employees have to investigate who made this mistake and why. That affects productivity and wastes time and energy. As illustrated in Figure 4, the most affected is productivity; therefore, it will affect the employee's energy when dealing with customers; they won't tend to have the passion to sell; therefore the atmosphere will have an impact on customers, and that will affect the reputation of the centre.

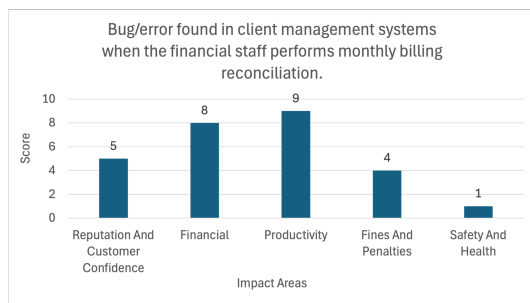


Figure 4: Risk Analysis - Area of Concern 2.

The following figure represents the impact areas of the possibility of vulnerability attacks by internal/external client management systems. The major vulnerability for this is the outdated system and not conducting regular system security management. Along with not assigning strong accounts passwords and strict authorization for each employee.

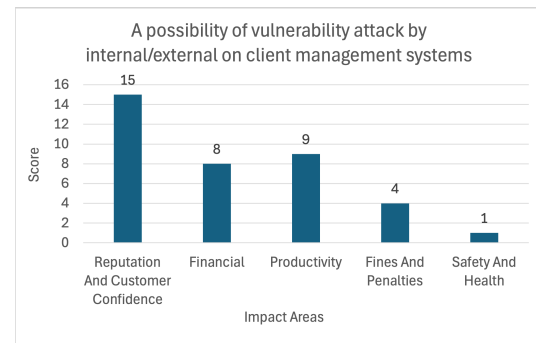


Figure 5: Risk Analysis - Area of Concern 3.

Because employees share accounts with third-party providers, that is a vulnerability along with an easily guessed password, which would lead to data leak, theft, or alteration of data. When employees leave the company, the IT does not update any passwords, and that is another vulnerability as illustrated in Figure 6; when this happened, it would affect the company's reputation majorly, and would lower the sales to affect the financial, and that would lead to affecting the productivity.

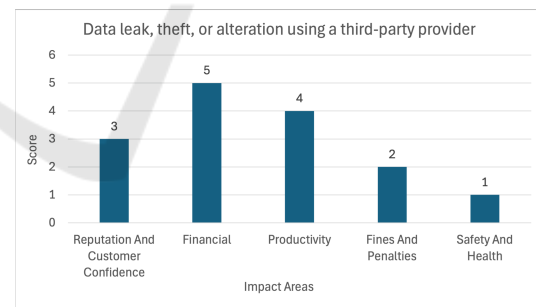


Figure 6: Risk Analysis - Area of Concern 4.

## 4.8 Step 8: Select Mitigation Approach

The proposed strategy plan to reduce the risk is: by setting the mitigation approach, based on the risk score applied to which pool, from Table 11 the Relative Risk Matrix, and then selecting the mitigation approach based on the pool number of the Table 12 Mitigation Approach. Pool 1 is assigned when the risk score is high, between 35 to 45. Pool 1's mitigation strategy is to mitigate, which underlines the necessity of taking immediate action

to mitigate the risk level. Pool 2 is assigned when the risk score is medium between 25 and 34. Pool 2's mitigation strategy is either deferred or mitigated, and It clarifies the necessity of taking immediate action or acting later. Lastly, pool 3 is if the risk score is low between 15 and 24. Pool 3's mitigation strategy is accepted. It emphasizes a willingness to accept circumstances.

Table 11: Relative Risk Matrix.

Relative Risk Matrix		
Risk Score		
35 TO 45	25 TO 34	15 TO 24
Pool 1	Pool 2	Pool 3

Table 12: Mitigation Approach.

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Defer / Mitigate
Pool 3	Accept

Based on the previous tables, Table 11 and 12, the risk score was calculated, and the pool of a mitigation approach was identified for each area of concern in Table 5. For a comprehensive overview, Figure 7 illustrates that each area of concern was mapped on the risk matrix that assesses risks according to their potential consequences and likelihood. The horizontal axis shows the potential consequences, ranging from "Negligible" to "Extreme", while the vertical axis shows likelihood, from "Rare" to "Certain." The matrix is color-coded to emphasize the level of concern of risk; the colour green represents low risk, yellow/orange is moderate risk, and red is high risk.

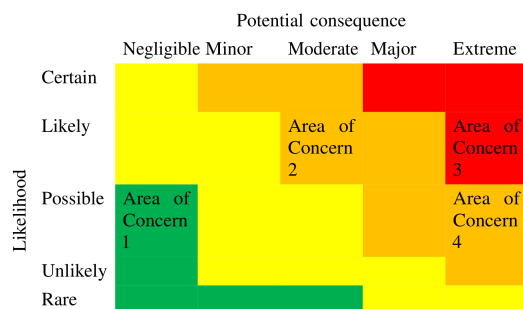


Figure 7: Risk Matrix: Likelihood vs. Consequences.

The following tables represent a detailed risk mitigation approach for each area of concern that was mentioned in Table 5 of Areas of Concerns. And underline the container and the control measures for each area of concern to help lower the likelihood of potential consequences.

Table 13: Risk Mitigation - Area of Concern 1.

Area of Concern	Errors in data input by customer service employees. Due to a large number of customers.
Relative Risk Score	30
Pool	Pool 2
Action Mitigate	Accept
Container	Client management systems, cloud storage, and billing systems
Control	Add validations for each field. If the system detects an error in the input data, the system prompts the user to correct the data right away. And it is conditioned to save and proceed.

Table 14: Risk Mitigation - Area of Concern 2.

Area of Concern	Bug/error found in client management systems when the financial staff performs monthly billing reconciliation
Relative Risk Score	16
Pool	Pool 3
Action Mitigate	Mitigate or defer
Container	Client management systems, cloud storage, and billing systems
Control	Add a confirmation popup and adjust the system interface to make it user-friendly to help employees avoid clicking incorrect buttons.

Table 15: Risk Mitigation - Area of Concern 3.

Area of Concern	A possibility of vulnerability attack by internal/external on client management systems
Relative Risk Score	15
Pool	Pool 1
Action Mitigate	Mitigate
Container	Client management systems, cloud storage, and billing systems
Control	Monitor periodically the system security to fix detected loopholes.

Table 16: Risk Mitigation - Area of Concern 4.

Area of Concern	Data leak, theft, or alteration using a third-party provider
Relative Risk Score	8
Pool	Pool 2
Action Mitigate	Mitigate or defer
Container	Client management systems, cloud storage, billing systems, and third-party providers.
Control	Create separate accounts for each employee, with a strong password that is periodically updated, and delete accounts of former employees.



## 5 LESSONS LEARNED AND RECOMMENDATIONS

In this step, we are proposing solutions and recommendations in response to the risks and threats identified by Diet Centre X to enhance security, productivity, financial and customer trust, and reputation. We recommend creating a customer registration system that is connected to the client management system, along with implementing a validation for each field to check on the entered data, instead of having the employee manually validate the customer data and copy it from Microsoft Office to the client management system. This process will narrow down the human errors and mistakes, and this will also save the employee time and energy, which the employee could use on something else, and will help the business save money instead of hiring an employee just to perform validation performance; the system will be handling that. We recommend that the company update and improve its billing system as it is outdated. There are payment options such as checks and visas, but the company does not accept visas, and neither do checks, regardless that no one uses checks at a diet centre, so this should be updated and removed; the system should be updated. Along with testing the interface to ensure that the interface is user-friendly, intuitive, and accessible to users of all skill levels. Additionally, conduct training sessions for employees whenever there is an established system update; employees should be trained on how to use newly updated interfaces. Conduct quarterly security awareness courses, along with conducting a real-time simulation to engage the employees to ensure that they are aware and prepared for facing potential security threats. Overall, conducting a comprehensive security awareness training program that is mandatory for all departments will help raise employees' awareness in matters of information security, as employees play a crucial role in maintaining the integrity of the business data. Diet Centre X needs to adopt a culture of security awareness across the centre to help minimize risks, threats, and vulnerabilities resulting from employee actions due to their lack of security training and awareness. Moreover, enforce quarterly password updates to help reduce exposure resulting from compromised passwords, in addition to establishing a system that automatically prompts users to update their passwords along with implementing a policy that expired passwords should not be reused or remain the same for a long period. In addition to implementing a password strength checker to ensure all new passwords must

be strong and difficult to guess, it must fulfil the requirements of complex passwords, which are It must be within at least 12 characters of lower and uppercase letters and a special character; a password strength checker should be conducted on all password updates to maintain strong passwords within all accounts of the company. These should be applied to client management systems, cloud storage, and third-party provider accounts. Lastly, we recommend implementing the framework approach used on the Diet Centre X on other small and medium-sized businesses to prove the effectiveness of the approach used on the Diet Centre X, we believe the approach used on the Diet Centre can be implemented on small and medium-sized business that has similar aspects as the diet centre where it does not mainly focus on the IT infrastructure and does not have special resources or experienced employees in the technical field. We believe that this type of small and medium-sized business could implement the same approach conducted on Diet Centre X and will mostly get an effective result as in Diet Centre X, the approach can be tailored to various industries of the small and medium-sized businesses.

## 6 CONCLUSIONS

In conclusion, we conducted a risk assessment using the OCTAVE Allegro framework to identify vulnerabilities at Diet Centre X, maintaining confidentiality by referring to it as Diet Centre X throughout the paper. We identified eight critical assets: employee profiles, customer profiles, subscriptions, customer health information, customer selections, and payment details. Four primary areas of concern emerged, each with proposed mitigation strategies based on risk scores. 1. 'Data Input Errors': Due to the high volume of customers, errors by customer service employees warrant accepting the risk. 2. 'Client Management System Bugs': Errors during monthly billing reconciliation suggest a choice to either accept or mitigate the risk. 3. 'Vulnerability Attacks': The risk of attacks on client management systems also allows for acceptance or mitigation. 4. 'Data Leaks via Third-party Providers': This risk requires active mitigation.

We analysed the potential impacts on productivity, legal compliance, financial stability, and reputation, establishing strategies to manage these risks effectively. Recommendations for Diet Centre X include implementing a customer registration system linked to management systems, upgrading the billing process, conducting regular security training, and

enforcing strict quarterly password updates. Finally, we suggest future research explore alternative frameworks for assessing Diet Centre X, comparing results to highlight more effective approaches.

## REFERENCES

- Chairopoulou, S. (2024). Cybersecurity in industrial control systems: a roadmap for fortifying operations. Master's thesis, Panepistimio Piraeus.
- Fahrurazi, M., Tarigan, S. A., Tanjung, M. A., and Mutijarsa, K. (2020). The use of iso/iec 27005: 2018 for strengthening information security management (a case study at data and information center of ministry of defence). In *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pages 86–91. IEEE.
- Herath, T. C., Herath, H. S., and Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, 25(2):681–721.
- Hillson, D. (2019). *Capturing upside risk: finding and managing opportunities in projects*. Auerbach Publications.
- Hom, J., Anong, B., Rii, K. B., Choi, L. K., and Zelina, K. (2020a). The octave allegro method in risk management assessment of educational institutions. *Aptisi Transactions on Technopreneurship (ATT)*, 2(2):167–179.
- Hom, J., Anong, B., Rii, K. B., Choi, L. K., and Zelina, K. (2020b). The octave allegro method in risk management assessment of educational institutions. *Aptisi Transactions on Technopreneurship (ATT)*, 2(2):167–179.
- Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons.
- Jhanjhi, N. Z. and Shah, I. A. (2024). *Navigating Cyber Threats and Cybersecurity in the Logistics Industry*. IGI Global.
- Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press.
- Miklian, J. and Hoelscher, K. (2022). Smes and exogenous shocks: A conceptual literature review and forward research agenda. *International Small Business Journal*, 40(2):178–204.
- Moore, W. and Frye, S. (2019). Review of hipaa, part 1: history, protected health information, and privacy and security rules. *Journal of nuclear medicine technology*, 47(4):269–272.
- Ozeer, U. and Pouye, B. (2021). Risk analysis based security compliance assessment and management for sensitive health data environment. In *2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM)*, pages 1–7. IEEE.
- Pearlson, K. E., Saunders, C. S., and Galletta, D. F. (2024). *Managing and using information systems: A strategic approach*. John Wiley & Sons.
- Putra, A. P. and Soewito, B. (2023). Integrated methodology for information security risk management using iso 27005: 2018 and nist sp 800-30 for insurance sector. *International Journal of Advanced Computer Science and Applications*, 14(4).
- Samonas, S. and Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).
- Suroso, J. S. and Fakhrozi, M. A. (2018). Assessment of information system risk management with octave allegro at education institution. *Procedia Computer Science*, 135:202–213.
- Ugbebor, F., Aina, O., Abass, M., and Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for sme contexts to reduce human-error related security incidents. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, 3(3):382–409.
- Van Devender, M. S. (2023). *Risk Assessment Framework for Evaluation of Cybersecurity Threats and Vulnerabilities in Medical Devices*. PhD thesis, University of South Alabama.