Allegro Worksheet 1	Risk Measurement Criteria – Reputation and Customer Confidence		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than 2% reduction in customers due to loss of confidence	2 to 5% reduction in customers due to loss of confidence	More than 5% reduction in customers due to loss of confidence
Other:			

Reputation

Low: For example, when a recent cyber incident occurred, ABC Technologies immediately sent out a notification to all affected customers, explaining what had happened and outlining the steps they were taking to resolve the issue. ABC Technologies, much like Google in 2019, can anticipate a minimal impact on reputation in the face of a minor disruption. Timely and effective resolution efforts, coupled with transparent communication, will mitigate any potential damage. For instance, Google's outage showcased that users quickly regain confidence when informed and reassured promptly (Google 2019).

Moderate: While it is possible for ABC Technologies to recover from such a scenario, it will require a considerable amount of effort and expense. To illustrate this, let's take a look at the infamous Equifax data breach that took place in 2017. This incident dealt a severe blow to Equifax's reputation and required them to put in substantial resources for recovery. It serves as an example of how disruptive events can have longlasting effects on a company's image and operations (Wang and Johnson 2018). For ABC Technologies, dealing with a major disruption would mean going through a similar journey. They would need to invest time,

money, and manpower to regain trust and get back on track. Rebuilding their reputation in the eyes of customers and stakeholders would be crucial for their long-term success.

High: If ABC Technologies faces a severe and prolonged incident, the impact on reputation could be irreversible. The aftermath of a major data breach, like the one experienced by Yahoo, serves as a cautionary example. Yahoo's breach not only damaged its reputation but also led to long-term consequences, including a decrease in user trust and a substantial reduction in the company's valuation (DIGISTOR 2022).

Customer Loss

Low: In 2017, Amazon faced a major web services outage that caused concern among its customers. However, ABC Technologies can take comfort in the fact that they can expect a minimal customer loss of less than 2% in the event of a minor disruption. The key lies in swift recovery efforts and transparent communication with customers. Amazon's experience serves as a valuable lesson for ABC Technologies. Despite the brief outage, Amazon managed to retain customer confidence by promptly resolving the issue and keeping customers informed about the situation. This transparent approach reassured customers and prevented widespread panic.

Moderate: In a scenario where the disruption is more significant, ABC Technologies might experience a customer loss between 2% and 5%. To put this into perspective, let's consider an example from Microsoft. In 2018, their gaming platform Xbox Live faced a similar situation. While there was a slight decrease in users, Microsoft was quick to communicate with their customers and resolve the issue efficiently. This proactive approach helped to minimize the impact on their user base. ABC Technologies recognizes the significance of staying connected with their customers and resolving any disruptions promptly to ensure their satisfaction remains high.

High: In the event of a severe and prolonged incident, ABC Technologies could face a customer loss exceeding 5%. As a result, Equifax experienced a significant decline in its customer base. This serves as a stark reminder to ABC Technologies of the importance of maintaining robust security measures and promptly addressing any breaches to avoid potential customer losses exceeding 5%. By learning from such incidents and taking proactive steps, ABC Technologies aims to protect its customers' trust and ensure their continued loyalty (Choi 2021).

Allegro Worksheet 2	**RISK MEASUREMENT CRITERIA – FINANCIAL**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 2% ($400,000) in yearly operating costs	Yearly operating costs increase by 2% to 10% ($400,000 to $2 million)	Yearly operating costs increase by more than 10% (over $2 million)

Revenue Loss	Less than 1% ($800,000) yearly revenue loss	1% to 5% ($800,000 to $4 million) yearly revenue loss	Greater than 5% (over $4 million) yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $100,000	One-time financial cost of $100,000 to $500,000	One-time financial cost greater than $500,000
Other:			

Before discussing the potential financial impact scenarios, it is necessary to establish hypothetical financial data for ABC Technologies. The assumed financial data for ABC Technologies is as follows: the net worth is $50 million, the current operating costs amount to $20 million per year, and the yearly revenue stands at $80,000,000 million per year.

Low Impact

In this low-impact, if ABC Technologies takes a proactive approach by implementing a cybersecurity awareness training program for employees. This initiative aims to enhance the workforce's ability to identify and respond to potential threats, thereby fortifying the company's overall cybersecurity posture.

Operating Costs: The operating costs of ABC Technologies have increased by less than 2%. This increase is primarily due to the expenses incurred for conducting the cybersecurity awareness training program. However, considering the company's strong financial position with a net worth of $50 million, it is capable of easily managing this slight rise in costs. The decision to invest in employee training is seen as a proactive approach to protect against potential cyber threats, making it a valuable and sensible allocation of resources.

Revenue Loss: The annual revenue loss is estimated to be less than 1%, which amounts to approximately $800,000. This projection assumes that prompt action is taken to address the cybersecurity incident and that customer trust remains unaffected. The minor decrease in revenue is deemed reasonable given the potential significant impact of a cybersecurity breach and the importance placed on maintaining a secure and trustworthy business environment. The revenue loss is viewed as a necessary expense to protect the company's long-term financial stability and reputation.

One-Time Financial Loss: A one-time cost of less than $100,000 for enhanced security measures is reasonable and aligns with the assumed financial capacity.

Moderate Impact

ABC Technologies encounters a moderate data breach that prompts the implementation of advanced cybersecurity measures. These measures include significant system upgrades and employee retraining, aiming to fortify the company's defenses against future cyber threats.

Operating Costs: The operating costs of ABC Technologies are expected to increase by 2% to 10%, equivalent to a range of $400,000 to $2 million. This increase is attributed to the implementation of advanced security measures, which incur additional expenses. ABC Technologies acknowledges the importance of allocating resources towards addressing these heightened costs. Despite the moderate impact on operating costs, the company believes it is manageable within their financial capabilities due to their commitment to enhancing cybersecurity resilience. Therefore, this investment is seen as a proactive measure aimed at preventing future breaches and safeguarding the overall integrity of the business.

Revenue Loss: The projected revenue loss resulting from the data breach is estimated to be between 1% and 5% per year, equivalent to a range of $800,000 to $4 million. This anticipated financial impact is a direct consequence of the breach's negative effect on customer trust and loyalty. ABC Technologies recognizes the significance of implementing strategic measures in order to recover from this moderate financial setback. To rebuild trust and minimize the impact on revenue, the company may allocate resources towards targeted marketing campaigns, customer communication initiatives, and additional customer support. Despite the substantial extent of the loss, ABC Technologies considers these efforts crucial for restoring customer confidence and ensuring long-term financial stability.

One-Time Financial Loss: Ranging from $100,000 to $500,000. The one-time financial loss represents the cost of addressing the immediate aftermath of the data breach. This includes expenses related to incident response, legal consultations, and any necessary compensations or reparations.

High Impact

If ABC Technologies faces a severe cybersecurity incident resulting in major security overhauls, significant system upgrades, and extensive employee retraining. The incident leads to the loss of important contracts and a substantial drop in customer confidence.

Operating Cost: The cybersecurity incident will necessitate extensive security measures, including system upgrades and employee retraining. These measures resulted in a more than 10% increase in operating costs, surpassing $2 million. ABC Technologies, grappling with the aftermath of the attack, had to allocate significant resources to fortify its security infrastructure. The costs associated with hiring cybersecurity

experts, implementing advanced security systems, and conducting extensive employee training contributed to the substantial increase in operating costs. This placed a strain on the company's financial resource, requiring strategic financial planning to manage the impact on its net worth.

Revenue Loss: The severe cybersecurity incident had a profound impact on customer trust, leading to a greater than 5% yearly revenue loss, exceeding $4 million. ABC Technologies witnessed a decline in customer confidence following the cybersecurity breach. The loss of important contracts and a substantial drop in sales contributed to a significant revenue downturn. Customers, concerned about the security of their data and the reliability of ABC Technologies' services, turned to alternative providers. In response, ABC Technologies implemented robust recovery strategies, such as rebuilding trust through transparent communication, enhancing security protocols, and offering incentives to regain lost clientele.

One-Time Financial Loss: A one-time financial cost greater than $500,000 for a high-impact incident indicates a substantial financial burden that would significantly impact ABC Technologies' financial health. The loss of crucial contracts has had a detrimental impact on ABC Technologies' financial standing, forcing them to make up for the sudden drop in revenue. This single financial setback amounted to over $500,000, placing a weighty burden on the company's resources.

The financial impact scenarios offered a structure for comprehending the possible outcomes of cybersecurity incidents for ABC Technologies. The events described in the case study, including difficulties related to growth, contract losses, and customer confidence issues, confirm that the scenarios align with the company's actual experiences. These scenarios underscore the significance of taking proactive cybersecurity measures and highlight the potential financial consequences for organizations operating in a technology-driven setting.

Allegro Worksheet 3	**RISK MEASUREMENT CRITERIA – PRODUCTIVITY**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 5% for 1 to 2 day(s).	Staff work hours are increased between 5% and 15% for 3 to 5 day(s).	Staff work hours are increased by greater than 15% for 7day(s) or more
Other: Customer Service	Slight impact on customer service; manageable customer inquiries	Moderate impact on customer service; requires additional support for inquiries	Significant impact on customer service; potential increase in customer complaints

Other:			
Other:			

Staff Hours

Low: A minor increase of less than 5% in staff work hours for 1 to 2 days represents a situation where ABC Technologies may encounter short-term demands or unexpected tasks. This minimal adjustment in work hours is manageable and is unlikely to significantly disrupt the regular workflow. Employees can accommodate this slight increase without major impact on productivity or work-life balance.

Moderate: An increase between 5% and 15% in staff work hours for 3 to 5 days signifies a more significant demand on the workforce. This level of impact might arise from sudden projects, urgent deadlines, or unforeseen challenges. While it could lead to a temporary adjustment in work hours, ABC Technologies should ensure proper support mechanisms, such as breaks and additional resources, to maintain productivity and prevent employee burnout during this moderately demanding period.

High: A high impact involves a substantial increase of more than 15% in staff work hours for 6 to 10 days. This scenario indicates a prolonged and intense demand on the workforce, potentially affecting employee well-being and overall productivity. It could be triggered by major projects, critical phases of development, or unforeseen operational challenges. The situation is made worse by the fact that website designer Julia Robinson missed a month of work due to illness, which indicates that there are no backup plans in place for staff absences. The workload is strained by this absence, which lowers morale and productivity. The entire situation casts doubt on the company's capacity to uphold a safe working environment, which affects trust in its operational resilience. To mitigate this impact, ABC Technologies must carefully manage workloads, consider temporary resource reinforcements, and implement strategies to safeguard employee health and morale during this demanding period.

Customer Service

Low: A slight impact on customer service, resulting from minor disruptions in productivity, is manageable. With an increase of less than 5% in staff work hours for 1 to 2 days, the customer service team can efficiently handle inquiries and maintain service levels. The impact on customer satisfaction is minimal, and the team can navigate the situation without a significant increase in customer inquiries.

Moderate: moderate impact on customer service, with a 5% to 15% increase in staff work hours for 3 to 5 days, may lead to a slightly higher volume of inquiries. The team may experience challenges in response

times and resource allocation. However, with additional support and coordination, ABC Technologies can ensure that customer inquiries are addressed effectively, minimizing the impact on customer satisfaction and maintaining a reasonable level of service quality.

High: A high impact on customer service, involving a greater than 15% increase in staff work hours for 6 to 10 days, poses significant challenges. This level of demand may lead to a substantial increase in customer inquiries, potentially impacting response times and overall service quality. ABC Technologies must implement robust strategies, such as additional staffing or streamlined communication channels, to ensure that customer satisfaction is preserved during this demanding period.

Allegro Worksheet 4	**RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH**		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

Other:			

Life

In the case of ABC Technologies, maintaining a commitment to life safety is paramount. For instance, a scenario where the alarm system in the Bradford office is not functional poses a direct threat to the lives of employees during emergency situations. The malfunction raises questions about the company's ability to ensure the safety of its staff members in critical situations. This underscores the importance of robust safety measures to safeguard lives.

Health

The case study highlights instances where staff members perform additional tasks beyond their formal roles. This can lead to increased stress levels and potential health issues, impacting the overall well-being of the workforce. Additionally, the absence of a clear policy and suitable environment for software development and testing may contribute to increased stress and potential health concerns among employees involved in these activities.

Safety

The malfunctioning alarm system in the Bradford office is a clear example of safety being questioned. This incident raises concerns about the overall safety infrastructure in the workplace.

Allegro Worksheet 5	Risk Measurement Criteria – Fines and Legal Penalties		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $2,000,000 are levied.	Fines between $2,000,000and $15,000,000are levied.	Fines greater than $15,000,000 are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $5,000,000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $5,000,00 and $15,000,000 are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $15,000,000 are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

ABC Technologies needs to comply with all legislation and regulations applicable to its operations. However, the absence of a definitive list of applicable legislation can potentially impact the company in terms of lawsuits, fines, and investigations. Without a clear understanding of the specific laws that apply to their industry and activities, ABC Technologies may unknowingly violate certain regulations. This could lead to legal disputes with regulatory authorities or individuals affected by non-compliance. Such lawsuits can be time-consuming, costly, and detrimental to the company's reputation (Walsh, 2023).

Furthermore, not having a comprehensive list of applicable legislation makes it difficult for ABC Technologies to ensure full compliance. This lack of clarity may result in unintentional non-compliance with certain regulations, which can attract fines from regulatory bodies. These fines could be substantial and have a direct impact on the company's financial health.

In 2018, Facebook faced significant legal challenges due to their unknowing violation of certain regulations. The absence of a definitive list of applicable legislation impacted the company's ability to fully comply with privacy laws, leading to lawsuits and investigations. The Cambridge Analytica scandal revealed that Facebook had unintentionally allowed personal data of millions of users to be harvested without their consent. This breach of privacy regulations resulted in numerous legal disputes with regulatory authorities and individuals affected by the non-compliance. The lawsuits were time-consuming, costly, and severely damaged Facebook's reputation. As a result, the company faced substantial fines from regulatory bodies and experienced a significant decline in its financial health. This serves as a cautionary example for companies like ABC Technologies to prioritize understanding and complying with all applicable legislation to avoid similar consequences (McCallum, 2022).

ABC Technologies' review of compliance with its policies, standards, and procedures is long overdue. Although no specific timeframe has been set for these reviews, they typically occur only when incidents or breaches take place. This reactive approach not only undermines the organization's commitment to maintaining compliance but also increases the likelihood of data breaches going undetected.

In relation to GDPR violations, ABC Technologies' failure to proactively review its compliance can result in severe financial penalties. Under GDPR regulations, organizations can be fined up to €20 million or 4% of their global annual turnover (whichever is higher) for serious infringements (Voigt & Bussche, 2017). The exact amount that ABC Technologies may have to pay would depend on various factors such as the nature and extent of the violation.

If ABC Technologies handles customer data improperly and incurring regulatory investigations, fines, and legal penalties due to their ignorance of specific data protection requirements and subsequent noncompliance with applicable legislation. There are two main ways in which this situation affects GDPR. First, it is difficult to guarantee compliance with the requirements of GDPR, which require organizations to respect certain rights and obligations when handling personal data, in the lack of a definitive list of applicable laws. Second, given that GDPR requires ongoing compliance assessments, there are concerns regarding the overdue review of policy, standards, and procedure compliance. Ignoring these reviews could result in the omission of possible GDPR violations, especially given the SaaS environment of ABCloud.

For organizations to protect themselves, proactive compliance with GDPR requirements is essential. For example, a company like Marriott was hit with mega millions fine of about $123millions for violating GDPR rules and regulations (O'Flaherty, 2019). This highlighting how important it is for organizations to set up safeguards against illegal access to customer and business information (Krause and Tipton, 2016) To maintain confidentiality and avoid fines, organizations must abide by GDPR, which mandates data protection measures based on the sensitivity of the data.

To avoid these potential consequences and safeguard customer trust, ABC Technologies must urgently prioritize a comprehensive review of its compliance framework.

Allegro Worksheet 6	**RISK MEASUREMENT CRITERIA – USER DEFINED**		
Impact Area	**Low**	**Moderate**	**High**

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	**IMPACT AREAS**
5	**Reputation and Customer Confidence:** ABC Technologies places the highest priority on maintaining a positive reputation and customer confidence. Any negative impact in this area can have long-lasting consequences, affecting customer trust and brand image.

4	**Financial**: Financial stability is crucial for ABC Technologies, but it is ranked slightly lower than Reputation and Customer Confidence. The company's growth, development plans, and ability to attract investors heavily depend on its financial standing. The case study highlights the significance of financial data, making it a high priority, but not the topmost concern.
2	**Productivity:** Productivity is a significant concern for ABC Technologies, especially given the complexities of software development and the interdependence of various teams. However, it is ranked lower than Reputation, Financial, and Legal aspects because disruptions in productivity, while impactful, may have more immediate and short-term effects compared to the long-term consequences associated with the top three priorities.
1	**Safety and Health:** Safety and Health, while important, are ranked the lowest in priority for ABC Technologies. The case study does not highlight specific safety or health risks that pose immediate and severe threats to the organization. The nature of ABC Technologies' business operations, primarily focused on software development and IT services, places safety and health lower in priority compared to other critical areas.
3	**Fines and Legal Penalties**: While legal consequences and fines are critical, they are ranked lower than Reputation and Financial aspects. ABC Technologies, being in the technology and software industry, understands the potential legal implications of data mishandling and non-compliance. However, immediate and severe legal consequences may be less frequent compared to ongoing concerns related to reputation and financial stability.
N/A	**User Defined**

This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Other third-party problems or systems	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 2 **Physical Containers**

This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire -2 (cont)	**Physical Containers**

Scenario 3:

In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 3	People

This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1:

Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?[1]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?[2]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[3]	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

[1] This case is unlikely, but if a key person in your organization has detailed knowledge of an information asset and communicates this information in an altered way that affects the organization, a risk could result.

[2] This case is about the availability of the information. If a key person in the organization has detailed knowledge that is vital for a business process and is not accessible or available, the information may not be usable for the purpose intended, ultimately impacting the organization.

[3] If a key person in the organization knows the information asset and leaves the organization, and the information is not documented elsewhere, it could pose a risk to the organization.

(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Product Source Code	The source code holds great significance for ABC Technologies as it distinguishes them from their rivals and embodies years of diligent effort, knowledge, and original thinking, thereby serving as a valuable and distinctive resource for the company. Devoid of the source code, ABC would be unable to create or sustain their CRM system, resulting in a diminished business and competitive edge.	The source code represents the proprietary set of instructions and statements written in a programming language that constitutes the fundamental building blocks of ABC Technologies' software applications and solutions. The source code is typically organized into files and directories, reflecting the structure of the software projects. It may include scripts, modules, libraries, and configuration files necessary for the development and functionality of the software.

(4) Owner(s)

Who owns this information asset?

Sam Gold

(5) Security Requirements

What are the security requirements for this information asset?

❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Sam Gold (Software Development Manager) Sally McCarty (Vice President) Paul Evans (President) Sabina (CEO) Debby Martinez (Analyst) Mick Harris (Software Programmer)
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Sam Gold (Software Development Manager)
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Mick Harris (Programmer)
	This asset must be available for 52 hours, 7days/week, 52weeks/year	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Central File Server: This essential server is the centralized hub for storing all critical information, such as orders, production records, and personnel data.	William Clay – IT Supervisor
2. Windows 10 Operating System: This is the operating system that employees use to access and work on the source code of the product.	William Clay – IT Supervisor
3. IT Network: The network infrastructure that links desktop computers, servers, and other devices at both the head office and sales office.	Peter Ly
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. ABCloud Cloud Environment: The cloud environment, where the software developed by ABC Technologies is stored	ABCloud
2. .	
3.	
4.	
5.	

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Corporate Office Building: This is the impressive structure that serves as the headquarters for ABC Technologies, where all business operations and offices are located.	

2. Central File Server The servers and infrastructure crucial for ABC Technologies' operations.	Alan Brown William Clay
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. ABCloud Data Centers: The physical facilities/locations where ABCloud's servers and infrastructure are situated.	ABCloud
2.	
3.	
4.	

Allegro Worksheet 9c	**INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)**
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
1. Mick Harris Actively involved in coding and scripting to develop software applications.	Software Activity Team
2. Sam Gold Oversee the entire software development team and projects. Set development goals, strategies, and ensure project timelines are met.	Software Activity Team
3. Alan Brown Develop and implement information security policies and procedures. Conduct risk assessments and implement security controls.	Software Activity Team

4. William Clay Oversee the overall IT infrastructure and operations. Manage the IT team, including network supervisors, helpdesk technicians, and support staff.	IT team
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	**ORGANIZATION**
1. ABCloud Support Engineer Providing 24/7 customer service support to ABC Technologies	ABCloud
2.	
3.	
4.	

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**		
Information Asset R	Information Asset	Product source code	
	Area of Concern	*Altering and destroying the original source code*	
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Internal Employees External Hackers	
	(2) Means *How would the actor do it? What would they do?*	Using weak access control and also	
	(3) Motive *What is the actor's reason for doing it?*	Internal employees have the potential to undermine operations and make unauthorized changes, while external hackers may seek to gain a competitive edge or cause disruptions. Both of these threats pose serious risks to the organization.	
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	Customers may lose confidence in their products, worrying that their personal data could be at risk. This lack of trust could result in customers leaving and choosing other brands instead. Not only would this hurt ABC Technologies financially, but it would also negatively impact their position in the market. The competition would gain an advantage, making it harder for ABC Technologies to recover its reputation and regain customer trust.	Reputation & Customer Confidence	High	10
		Financial	Medium	5
	This could lead to legal liabilities, as customers may suffer financial losses or damages and seek compensation through lawsuits. Not only that, but imagine the nightmare of having to recall a product because of its vulnerabilities! The financial burden would be immense.	Productivity	low	3
		Safety & Health	low	2
		Fines & Legal Penalties	medium	6
		User Defined Impact Area		
			Relative Risk Score	**26**

(9) Risk Mitigation
Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*

REFERENCES

Adubato, S. (2020) Johnson & Johnson's Tylenol Scare. GETTING IT RIGHT. *What Were They Thinking?* Rutgers University Press. 12–19.

Choi, Y.B. (2021) Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases. *International Journal of Cyber Research and Education* 3 (1), 58–64.

DIGISTOR (2022) *What Happens to a Company's Reputation After a Data Breach?* https://digistor.com/what-happens-to-a-companys-reputation-after-a-data-breach/ Accessed 13 January 2024.

Google (2019) *Google Cloud Status Dashboard*. https://status.cloud.google.com/incident/cloudhttps://status.cloud.google.com/incident/cloud-networking/19009%20Accessed%2013%20January%202024networking/19009 Accessed 13 January 2024.

Krause, M. and Tipton, H.F. (2016) *Information Security Management Handbook, Volume 5*. CRC Press.

McCallum, B.S. (2022) *Meta settles Cambridge Analytica scandal case for $725m*. https://www.bbc.co.uk/news/technology-64075067 Accessed 13 January 2024.

Morello, L. (2015) BP agrees to pay US$18.7 billion to settle Deepwater Horizon oil-spill claims. *Nature* .

Nozaki, M.K. and Tipton, H.F. (2016) *Information Security Management Handbook, Volume 5*. CRC Press.

O'Flaherty, K. (2019) Marriott Faces $123 Million Fine For 2018 Mega-Breach. *Forbes* 9 July.

Voigt, P. and Bussche, A. von dem (2017) *Enforcement and Fines Under the GDPR*. https://link.springer.com/chapter/10.1007/978-3-319-57959-7_7 Accessed.

Walsh, K. (2023) Compliance Risk. *Security-First Compliance for Small Businesses* Boca Raton: CRC Press. 39–56.

Wang, P. and Johnson, C. (2018) CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH. *Issues In Information Systems* .