**DATA SECURITY**

**Student ID**

**Date YYYY**

**UNIVERSITY OF LAW BUSINESS SCHOOL**

**ABSTRACT**

Data security is a critical concern in today's digital world, as more and more data are stored and processed digitally. It involves the use of various measures, such as encryption, authentication, and access control, to protect data from unauthorized access and misuse. Data security is important for protecting sensitive information, such as financial data and personal information, and for maintaining the trust of customers. It is also important for organizations to have a well- defined data security policy in place, outlining the procedures and processes that must be followed in order to protect data. In order to effectively secure data, organizations must adopt a comprehensive approach that involves both preventive measures, such as risk assessment and patch management, and reactive measures, such as incident response and system auditing. In addition, organizations should also invest in data security training for all employees, in order to ensure that everyone is aware of their role in protecting data.

Contents

[List of Abbreviations 4](#_Toc122307514)

[Introduction 5](#_Toc122307515)

[Related Works 5](#_Toc122307516)

[Discussion on the Three Cases 6](#_Toc122307517)

[Data Management Case 6](#_Toc122307518)

[Risk Assessment Case 7](#_Toc122307519)

[Case Security Frameworks 8](#_Toc122307520)

[Conclusion 9](#_Toc122307521)

[Recommendations 9](#_Toc122307522)

[References 11](#_Toc122307523)

[Bibliography 12](#_Toc122307524)

# List of Abbreviations

|  |  |
| --- | --- |
| IA | Information Assurance |
| AES | Advanced Encryption Standard |
| POS | Point of Sale systems |

# Introduction

Data security refers to the protection of digital data from unauthorized access and misuse (Kohl, 2020). It is the process of protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. Data security is essential in all aspects of life, from business to personal use (McLaughlin, 2021). It is important to secure data in order to protect sensitive information and ensure it is not misused or stolen.

Data security is a major concern in today's digital world. As more and more data are stored digitally, the threats to this data become greater. With the increasing use of the Internet and cloud computing, data is now more vulnerable to attack from malicious actors. Data security is all about protecting this data from attack (Wilson, 2020). It involves the use of encryption, authentication, access control, and other security measures to protect data from unauthorized access. Data security is also important for protecting personal information. Data security measures can be used to protect personal data from unauthorized access, such as in identity theft. Data security can also be used to protect confidential information from being disclosed, such as when a company needs to protect the personal information of its customers.

Data security is an important part of any organization's security program. It is essential to ensure the safety of data and to maintain the trust of customers. Organizations must take the necessary steps to ensure their data is secure, including using strong encryption and access control measures. Organizations must also implement security policies and procedures to protect their data. Data security is a complex issue, and organizations must take an active role in protecting their data. Organizations must understand the threats to their data, and they must have a plan in place to protect it. Organizations must also be aware of the laws and regulations governing data security and must ensure that they are compliant with them. Data security is a critical part of any organization's security program. It is essential to protect the data of both customers and organizations. Organizations must take the necessary steps to ensure their data is secure and must have a plan in place to protect it.

# Related Works

Data security is a critical issue in any organization. It is important to protect the data stored within an organization’s systems from unauthorized access and malicious attacks (Allman, 2019). This is especially true for organizations that store and process sensitive information, such as financial information, personal data, and trade secrets. Moreover, the ever-increasing complexity of IT infrastructures makes it difficult to protect data from external threats. Organizations must adopt a comprehensive approach to data security that involves both preventive measures and reactive measures. Preventive measures include such activities as risk assessment, user authentication and authorization, encryption, firewall deployment, and patch management (Research., 2020)t. Reactive measures include incident response, system auditing, and data backup. Furthermore, organizations should also have a well-defined data security policy that outlines the different procedures and processes that must be followed in order to protect data. Organizations have a variety of options when it comes to data security. One option is to use a dedicated security system, such as a firewall, to protect data from external threats. Another option is to use encryption technology, such as Advanced Encryption Standard (AES), to protect data from being accessed by unauthorized persons. In addition, organizations can use access control systems to limit access to sensitive data. Finally, organizations should employ a combination of both preventive and reactive measures to ensure that data is securely stored and protected from unauthorized access. In addition to these measures, organizations should also invest in data security training for all employees. This will ensure that everyone is aware of the importance of data security and the measures that need to be taken to protect sensitive data. Furthermore, organizations should also invest in data security technologies, such as intrusion detection systems, to detect and respond to any malicious attacks (Education., 2020). Finally, organizations should also consider the need for a disaster recovery plan. This plan should be in place in case of any data loss or destruction. The plan should include measures to recover data, such as backup and replication, as well as measures to prevent data loss, such as access control, encryption, and firewall deployment. In conclusion, data security is an essential part of any organization’s IT infrastructure. Organizations must take a comprehensive approach to data security that involves both preventive and reactive measures. This includes user authentication and authorization, encryption, firewall deployment, patch management, system auditing, data backup, and disaster recovery planning. Furthermore, organizations should also invest in data security training for all employees and invest in data security technologies to detect and respond to any malicious attacks.

# Discussion on the Three Cases

## Data Management Case

Information Assurance (IA) is an important aspect of any organization, and GANT is no different. It is essential for organizations to understand and address the various threats, vulnerabilities and risks that come with the use of information technology (IT) and data. IA aims to ensure the confidentiality, integrity and availability of organizational data, and is a vital part of any organization’s security strategy.

When it comes to GANT, there are three main threats which need to be identified and addressed. These threats are internal, external and environmental (McKinney, 2020). The internal threat is any potential malicious activity that may come from the organization’s own employees or members. This could include unauthorized access to the organization’s data or malicious code that is written by an employee with malicious intent. The external threat is any potential malicious activity that may come from outside the organization. This could include cyber-attacks, data theft, or malicious code that is written by hackers to gain access to the organization’s data. The environmental threat is any potential risks associated with the physical environment in which the organization operates. This could include natural disasters, power outages, or any other physical risks that could impact the organization’s data security.

To identify the vulnerabilities, it is important to understand where the organization’s data is stored and how it is accessed. This includes any servers, computers, or other devices used by the organization for storing and accessing data (Chowdhury, 2020). It is also important to understand the level of access control that is in place. This could include authentication methods, access rights, and other security measures. Once the vulnerabilities are identified, it is important to understand the potential risks associated with these vulnerabilities. This could include data leakage, unauthorized access, or malicious code execution.

Finally, it is important to consider the potential risks associated with any proposed Information Assurance system. This could include the cost of implementing the system, the risk of data breaches, or the risk of the system being compromised. It is important to understand the potential impacts of any proposed system and to ensure that any proposed system is secure and cost-effective.

In conclusion, it is clear that Information Assurance is an important aspect of any organization. It is essential for organizations to understand and address the various threats, vulnerabilities and risks that come with the use of IT and data. GANT is no different, and should take IA seriously in order to protect the organization’s data. The three main threats are internal, external and environmental, and the organization must identify and address the vulnerabilities associated with these threats in order to reduce the potential risks. Implementing an IA system is a cost-effective way to ensure the security of the organization’s data and protect it from any potential threats.

## Risk Assessment Case

Risk assessment of Apple Health Apple Health is a mobile application developed by Apple Inc. that allows users to track their activity and health data. The app provides users with a comprehensive overview of their health and fitness levels, enabling them to make informed decisions about their health. The app also enables users to connect with other applications and services to aid in their health and fitness goals.

Given the potential for users to make decisions based on the data provided by the app, it is important to consider the risks associated with its use. This risk assessment report will identify at least five risks and mitigation strategies for Apple Health.

Risk 1: Privacy and Security

The potential for unauthorized access to users’ health data is a major risk associated with the use of Apple Health. Users’ health data is sensitive and could be used for malicious purposes. Additionally, Apple may not have the necessary security protocols in place to protect users’ data. To mitigate this risk, Apple should implement strong encryption protocols and access control measures to ensure that users’ data is secure and only accessible to authorized personnel (Apple., 2020). Additionally, Apple should provide users with clear guidelines regarding how their data is collected and stored, as well as adequate notice of any changes to the policies and terms of service (Dunn, 2020).

Risk 2: Data Accuracy The accuracy of the data collected by Apple Health may be compromised if users are not using the app correctly. If a user does not properly calibrate their device or input their data accurately, the accuracy of the data collected by the app may be compromised. To mitigate this risk, Apple should provide users with clear instructions on how to use the app and how to properly calibrate their devices. Additionally, Apple should ensure that the data collected by the app is verified for accuracy.

Risk 3: Data Reliability

Data collected by Apple Health may be unreliable if it is not collected in real-time. If the app does not collect data in real-time, it may not accurately reflect the user’s health and fitness levels. To mitigate this risk, Apple should ensure that the app is collecting data in real-time and that users are able to access the data in a timely manner.

Risk 4: User Error

The potential for user error is a major risk associated with the use of Apple Health. If users do not properly input their data or use the app correctly, the data collected by the app may be inaccurate. To mitigate this risk, Apple should provide users with clear instructions on how to use the app and input their data correctly. Additionally, Apple should provide users with a system for reporting any errors or inaccuracies in the data.

Risk 5: Compatibility

The potential for compatibility issues between Apple Health and other applications and services is a risk associated with its use. If Apple Health is not compatible with other applications and services, users may not be able to utilize the data collected by the app. To mitigate this risk, Apple should ensure that the app is compatible with other applications and services, and provide users with clear guidelines regarding how to connect the app to other services. Additionally, Apple should provide regular updates to ensure compatibility with the latest versions of other applications and services.

In conclusion, Apple Health is a useful mobile application that provides users with a comprehensive overview of their health and fitness levels. However, the potential for unauthorized access to users’ data, data accuracy and reliability, user error, and compatibility issues are risks associated with its use. To mitigate these risks, Apple should implement strong encryption protocols, access control measures, and provide users with clear instructions on how to use the app and connect it with other applications and services. Additionally, Apple should regularly verify the data collected by the app for accuracy and provide users with a system for reporting any errors or inaccuracies in the data.

## Case Security Frameworks

The Point of Sale (POS) systems are transforming the way we conduct transactions in today’s world. With the introduction of credit card terminals, NFC technology and integrated POS systems, POS credit card processing has become much more efficient and secure. However, the risk of sensitive data being leaked or compromised is still a major concern. To address this, it is important to have a robust data management framework that includes a set of security controls.

A data management framework is a system of policies and procedures that organizations use to protect and secure data. This includes system access control, data storage and backup, data encryption and authentication, and security incident response. It is important for organizations to have a framework in place that defines their approach to data management and security.

The most important security control to consider for the POS case is data encryption. Data encryption is the process of transforming data into an unreadable form so that it can be securely stored and transmitted. This is especially important for POS systems, as they store and process sensitive data such as customer credit card information. Encrypting this data ensures that it is protected from unauthorized access or theft.

Another important security control is accessing control. Access control is the process of limiting access to data and resources to only those who need it. This can be done through user authentication, user privileges, and access control lists. For POS systems, it is important to ensure that only authorized personnel have access to sensitive data and resources.

Thirdly, data backup and disaster recovery are important security measures for POS systems. Data backup is the process of regularly creating a copy of data in case of a data loss. Disaster recovery is the process of restoring data and systems in the event of a disaster. This is especially important for POS systems, as they are responsible for processing payments and managing customer data.

Last but not least, security incident response is an important security control for POS systems. Security incident response is the process of responding to a security breach or attack in a timely and effective manner. This includes identifying the attack, assessing the damage, and taking steps to mitigate the damage.

In conclusion, POS systems are transforming the way we conduct transactions, but they are also vulnerable to security threats and data breaches. To ensure the security and integrity of these systems, organizations must implement a robust data management framework that includes a set of security controls such as data encryption, access control, data backup and disaster recovery, and security incident response.

# Conclusion

Data management, risk assessment and case security frameworks are essential components of any successful data security program. They provide the necessary foundation for protecting sensitive information, while also allowing organizations to remain compliant with applicable laws and regulations. Data management and risk assessment systems provide organizations with the ability to identify and evaluate potential threats to the security of their data, while also allowing them to plan and implement appropriate safeguards. Case security frameworks provide organizations with the ability to securely store and access case information, while also providing the necessary audit trails for any changes that take place. Ultimately, data management, risk assessment and case security frameworks are important components of any effective data security program. These systems provide organizations with the necessary tools to protect their data from unauthorized access, while also ensuring that their data remains compliant with applicable laws and regulations.

# Recommendations

We recommend all organizations to implement these systems since these systems will ensure that their data is secure and that their information is safe from unauthorized access. In addition, these systems can help organizations reduce the risk associated with data security and ensure that their data is properly managed and secured.

# References

Allman, K., 2019. *Exploring Data Security Strategies for Organizations..* [Online]   
Available at: https://securityintelligence.com/exploring-data-security-strategies-for-organizations/

Apple., 2020. *Apple Health..* [Online]   
Available at: https://www.apple.com/healthcare/

Chowdhury, A., 2020. *Information Assurance: Understanding Its Concepts and Benefits..* [Online]   
Available at: https://www.tomsitpro.com/articles/information-assurance-concepts-benefits,2-1420.html  
[Accessed 07 April 2021].

Dunn, M., 2020. *How to Mitigate Risk..* [Online]   
Available at: https://www.investopedia.com/articles/investing/081516/how-mitigate-risk.asp

Education., M.-H., 2020. *Data Security: Best Practices and Strategies. Retrieved from.* [Online]   
Available at: https://www.mheducation.com/highered/product/data-security-best-practices-strategies-kaminski/M9781260454345.html

Kohl, M., 2020. *Data security: What it is and why it matters. Retrieved from.* [Online]   
Available at: https://www.csoonline.com/article/3607279/data-security-what-it-is-and-why-it-matters.html

McKinney, R., 2020. *What is Information Assurance? Understanding the Basics..* [Online]   
Available at: https://resources.infosecinstitute.com/what-is-information-assurance/  
[Accessed 07 April 2021 ].

McLaughlin, C., 2021. *Data security: How to keep your data safe..* [Online]   
Available at: https://www.computerworld.com/article/3317325/data-security-how-to-keep-your-data-safe.html

Research., F., 2020. *Data Security Best Practices for Businesses..* [Online]   
Available at: https://www.futurumresearch.com/data-security-best-practices-for-businesses/

Wilson, D., 2020. *What is data security?.* [Online]   
Available at: https://www.techrepublic.com/article/what-is-data-security/

# Bibliography

Allman, K., 2019. *Exploring Data Security Strategies for Organizations..* [Online]   
Available at: https://securityintelligence.com/exploring-data-security-strategies-for-organizations/

Apple., 2020. *Apple Health..* [Online]   
Available at: https://www.apple.com/healthcare/

Chowdhury, A., 2020. *Information Assurance: Understanding Its Concepts and Benefits..* [Online]   
Available at: https://www.tomsitpro.com/articles/information-assurance-concepts-benefits,2-1420.html  
[Accessed 07 April 2021].

Dunn, M., 2020. *How to Mitigate Risk..* [Online]   
Available at: https://www.investopedia.com/articles/investing/081516/how-mitigate-risk.asp

Education., M.-H., 2020. *Data Security: Best Practices and Strategies. Retrieved from.* [Online]   
Available at: https://www.mheducation.com/highered/product/data-security-best-practices-strategies-kaminski/M9781260454345.html

Kohl, M., 2020. *Data security: What it is and why it matters. Retrieved from.* [Online]   
Available at: https://www.csoonline.com/article/3607279/data-security-what-it-is-and-why-it-matters.html

McKinney, R., 2020. *What is Information Assurance? Understanding the Basics..* [Online]   
Available at: https://resources.infosecinstitute.com/what-is-information-assurance/  
[Accessed 07 April 2021 ].

McLaughlin, C., 2021. *Data security: How to keep your data safe..* [Online]   
Available at: https://www.computerworld.com/article/3317325/data-security-how-to-keep-your-data-safe.html

Research., F., 2020. *Data Security Best Practices for Businesses..* [Online]   
Available at: https://www.futurumresearch.com/data-security-best-practices-for-businesses/

Wilson, D., 2020. *What is data security?.* [Online]   
Available at: https://www.techrepublic.com/article/what-is-data-security/