**DATA SECURITY**

**Student ID**

**Date YYYY**

**UNIVERSITY OF LAW BUSINESS SCHOOL**

**ABSTRACT**

Cyber threats are an ever-increasing concern in today’s digital world. As more organizations and individuals store their data and information online, the risk of data theft and misuse is increasing. This paper discusses three case studies focusing on data security and risk assessments. The first case study focuses on the Group for the Appreciation of the Natterjack Toad (GANT) and the need for information assurance to protect the group’s activities, meetings, website and other aspects of its work. The second case study looks at Apple Health, a healthcare product which collects and monitors the user’s health data. The third case study examines point of sale credit card processing and integrated POS systems. All three cases involve the potential risks associated with data storage, security, and management. By understanding the threats and vulnerabilities in each case, effective security controls can be implemented to mitigate risk and ensure the safety of the data. The findings from the three case studies show the importance of data security and the need for organizations to consider data management frameworks and risk assessment reports to protect their data and information.

Contents

[List of Abbreviations 4](#_Toc122953106)

[Introduction 5](#_Toc122953107)

[Literature Review 5](#_Toc122953108)

[Discussion on The Cases 6](#_Toc122953109)

[Data Management Case 6](#_Toc122953110)

[Risk Assessment Case 7](#_Toc122953111)

[Data Security and Privacy 8](#_Toc122953112)

[System Reliability 8](#_Toc122953113)

[Data Accuracy 8](#_Toc122953114)

[User Experience 8](#_Toc122953115)

[Third-Party Integration 8](#_Toc122953116)

[Regulatory Compliance 8](#_Toc122953117)

[Case Security Frameworks 9](#_Toc122953118)

[Conclusion 10](#_Toc122953119)

[Recommendations 10](#_Toc122953120)

# List of Abbreviations

|  |  |
| --- | --- |
| IA | Information Assurance |
| IAS | Information Assurance system |
| POS | Point of Sale systems |
| GANT | Group for the Appreciation of the Natterjack Toad |

# Introduction

This paper discusses the different assessment of three cases; the Group for the Appreciation of the Natterjack Toad (GANT) scenario, the Apple Health scenario, and the Point of Sale (POS) credit card processing scenario. It provides an insight into the risk assessment and data management frameworks for each of the three cases. The Group for the Appreciation of the Natterjack Toad (GANT) is a conservation group which is keen to promote and preserve the well-being of the Natterjack toad. The Apple Health is one of the best healthcare application examples that patients can use to get a better idea of their health. The Point of Sale (POS) credit card processing provides a simple and reliable way to accept credit cards at the point of sale.

The purpose of this paper is to provide an overview of risk assessment and data management frameworks for the three cases mentioned above. First, the paper will discuss the threats, vulnerabilities, and risks of the Group for the Appreciation of the Natterjack Toad (GANT) scenario. Second, it will provide a risk assessment report for the Apple Health scenario, including identifying five risks and corresponding mitigation strategies. Lastly, it will discuss the data management frameworks and security controls for the POS case. The scope of this paper is to provide an overview of risk assessment and data management frameworks for the three cases mentioned above. It will look at the threats, vulnerabilities, and risks of the GANT scenario, the risk assessment report for the Apple Health scenario, and the data management frameworks and security controls for the POS case.

This paper will discuss the risk assessment and data management frameworks for the three cases mentioned above. It will look into the threats, vulnerabilities, risks, and mitigation strategies for the GANT scenario, the Apple Health scenario, and the POS credit card processing scenario. The paper will conclude with a summary of the findings and recommendations for each of the three cases.

Literature Review

Information assurance is a critical component of the security of any organization, especially for organizations like GANT that rely heavily on their internet-based applications and networks. The first step in establishing an effective information assurance system is to identify the potential threats that the organization may face. Common threats to information assurance include unauthorized access to information, malicious attacks such as malware and phishing, data loss or corruption, and data breaches (Kuo, et al., 2017). Once the threats have been identified, the next step is to identify the organization’s vulnerabilities and the potential risks associated with them. Vulnerabilities can include weak passwords, insecure networks, lack of encryption, and inadequate training (Hu, et al., 2017). By identifying and evaluating these threats, vulnerabilities, and risks, organizations can develop an effective information assurance system.

Data security is a critical component of any healthcare application, particularly those that collect and store sensitive patient health data. To ensure that Apple Health is secure, it is important to identify and mitigate potential risks. One risk is unauthorized access to the application. This can be mitigated by using strong passwords and two-factor authentication and by restricting access to the application to authorized users only. Another risk is data leakage, which can be mitigated by using encryption, monitoring the application for suspicious activities, and ensuring that data is backed up and stored in a secure location. A third risk is malicious attacks, which can be mitigated by using secure firewalls, conducting regular security audits, and providing staff with adequate security training. Finally, a fourth risk is data breaches, which can be mitigated by implementing strict access control policies, regularly monitoring for suspicious activities, and ensuring that data is securely stored.

The security of point-of-sale credit card processing systems is a critical concern for organizations, as these systems are vulnerable to malicious attacks, data breaches, and other security risks. To ensure the security of these systems, organizations should implement a security framework that includes the proper controls, processes, and procedures. A common security framework for point-of-sale systems is the Payment Card Industry Data Security Standard (Ataya, 2010).This standard provides guidelines for the secure handling of credit card data by organizations. It establishes requirements for security policies, technology, and processes, including encryption, access control, and auditing. Additionally, organizations should implement additional security measures, such as multi-factor authentication, intrusion detection systems, and regular security audits, to ensure the security of their point-of-sale systems.

# Discussion on The Cases

## Data Management Case

According to (Acharya, 2020), Information Assurance is a set of practices, processes and policies that work together to protect an organization’s data and systems from unauthorized access, misuse, and destruction. It is essential for organizations such as GANT to have an Information Assurance system (IAS) in place since they handle sensitive data and have a large number of members in multiple countries. It is paramount for organizations to understand and address the various threats, vulnerabilities and risks that come with the use of information technology (IT) and data. Below are the threats, vulnerabilities and risks which GANT as an organization must work on to ensure they safeguard their sensitive data.

Threats posed by not having an Information Assurance system in place include data breaches, malicious attacks, and hacking. Data breaches can occur when confidential information is accessed without authorization. Malicious attacks involve the use of malicious software to gain access to an organization’s systems or data. Hacking can occur when an unauthorized user attempts to gain access to an organization’s systems or data. Also, Natural disasters such as floods, earthquakes, and hurricanes can cause physical damage to GANT's systems and potentially cause data to be lost or destroyed. This can cause significant disruption to the organization’s operations and data. (Kumar, et al., 2020)

Vulnerabilities that could contribute to a data breach, malicious attack, or hacking include Poor system security measures, Inadequate data protection measures and Poor physical security measures. Poor system security measures such as weak passwords, lack of two-factor authentication, and inadequate system access controls can leave GANT's systems vulnerable to attack or unauthorized access (Tuttle & Parise, 2017). Inadequate data protection measures such as lack of encryption, lack of data backups, and lack of data security policies can leave GANT's data vulnerable to being stolen or leaked (Meer, 2020). Poor physical security measures such as a lack of security cameras, lack of access control systems, and lack of physical security personnel can leave GANT's physical systems and data vulnerable to theft or vandalism (Kumar, et al., 2020). Other vulnerabilities include lack of employee training, outdated software, and lack of security protocols. Employees may not be aware of the importance of information security, or the risks associated with not having an Information Assurance system in place. Outdated software may contain security flaws that hackers can exploit. Finally, a lack of security protocols can leave an organization vulnerable to attack.

The risks associated with not having an Information Assurance system in place include damage to reputation, financial, and legal liabilities (Gorla, 2019). Financial risks such as loss of revenue, increased costs, and legal liabilities can result from malicious attacks, unauthorized access, or natural disasters. (Scherr, 2019). Reputational risks such as damage to the organization’s reputation, loss of customers, and decreased public trust can result from malicious attacks, unauthorized access, or natural disasters (Meer, 2020). Operational risks such as disruption to the organization’s operations and decreased efficiency can result from malicious attacks, unauthorized access, or natural disasters (Kumar, et al., 2020). If an organization’s data or systems are breached, their reputation may be damaged. This can lead to a loss of customers and a decrease in revenue. The organization may also be liable for any losses suffered by those whose data was compromised.

Lack of an Information Assurance system can pose a serious threat to GANT as we have discussed above. Without an Information Assurance system, GANT is vulnerable to data breaches, malicious attacks, and hacking. This can lead to financial losses, damage to reputation, and legal liabilities. With an Information Assurance system in place, GANT can protect their data and systems from unauthorized access and ensure that their members’ data is secure.

## Risk Assessment Case

Risk Assessment Report for Apple Health

Apple Health is an application created by Apple Inc. for tracking and monitoring the user’s health and activities (Apple., 2020). It monitors sleep, food, activity, heart rate, and other data that provides a comprehensive assessment of the user’s health data. It is one of the most comprehensive health applications available to users and provides an easy way to track and monitor health data. Risk assessment is the process of evaluating potential risks and vulnerabilities in order to determine the likelihood and severity of those risks. In the case of Apple Health, there are a number of potential risks and vulnerabilities that need to be identified and addressed. In order to provide an appropriate risk assessment report for this scenario, we must identify and analyze the following risks and mitigation strategies:

### Data Security and Privacy

Apple Health app collects and stores sensitive large amounts of personal health data collected from users, which is potentially vulnerable to unauthorized access and misuse. These large amounts of personal health data raise concerns about data security and privacy. To mitigate this risk, Apple must ensure that personal health data is protected by robust security measures, such as encryption of the data, access control, and authentication to prevent unauthorized access to the data (Ferrari, 2018). Furthermore, the Apple company should consider using two-factor authentication to further enhance the data security. Apple must ensure that only authorized personnel are able to access the data, and that all personal health data is securely deleted if it is no longer needed.

### System Reliability

Apple Health is a complex system, and any issues with the system’s reliability can lead to inaccurate and inconsistent data. To mitigate this risk, Apple must ensure that all components of the system are properly tested and maintained. Additionally, Apple must provide support and maintenance services to address any issues that may arise.

### Data Accuracy

The accuracy of the data collected and processed through the Apple Health app is essential for the successful use of the app. To mitigate this risk: Apple should ensure that the data collected and processed through the Apple Health app is accurate and reliable (Mishra, 2020). To do so, Apple should consider implementing measures such as regular testing and validation of the data, validation of the data sources, and continuous monitoring of the data accuracy. Additionally, Apple should ensure that the data collected through the Apple Health app is regularly reviewed and updated.

### User Experience

Apple Health must provide a user-friendly experience in order to be successful. If the user experience is not up to par, users may be discouraged from using the application. To mitigate this risk, Apple must ensure that the user experience is easy to use and intuitive. Additionally, Apple must provide support and troubleshooting services to address any user issues.

### Third-Party Integration

Apple Health integrates with a number of other applications and systems, and any issues with the integration can lead to data integrity issues. To mitigate this risk, Apple must ensure that all third-party applications and systems are properly tested and maintained. Additionally, Apple must ensure that all data is transferred securely and without errors.

### Regulatory Compliance

Apple Health must comply with applicable laws and regulations in order to operate legally. To mitigate this risk, Apple must ensure that the application is compliant with the relevant regulations and laws. Additionally, Apple must regularly review and update the application to ensure that it remains compliant.

Risks and mitigation strategies that we have identified above provide a comprehensive overview of the potential risks and vulnerabilities associated with Apple Health. By properly addressing these risks and vulnerabilities, Apple can ensure that the application is secure and reliable, and that users have a positive experience.

## Case Security Frameworks

Data management frameworks are essential for ensuring the safety and security of data and information associated with point of sale (POS) credit card processing (Bosco, 2020). It is important to consider various components of the framework, such as data privacy, data storage, data security, data integrity, data access control, and data protection.

Data privacy refers to protecting customer data from unauthorized access. It is important for businesses to implement data privacy measures, such as encryption and access control, to ensure that customer data is not accessible to anyone outside of the organization (Khandelwal, 2020). Additionally, businesses should ensure that customer data is not shared with third parties without customer consent. Data storage is another important component of the data management framework. Data must be stored securely, and businesses should ensure that data is stored in a secure manner, such as on a secure server or cloud. Additionally, businesses should ensure that customer data is stored in a way that is easily retrievable.

Data security is also essential for ensuring the safety and security of customer data. Businesses should ensure that their systems are equipped with the latest security measures, such as firewalls, antivirus software, and encryption. Additionally, businesses should ensure that their systems are regularly patched and updated in order to protect customer data from potential threats. Data integrity is also important for ensuring the accuracy and completeness of customer data. Businesses should ensure that data is stored in an accurate and consistent manner, and that any changes to customer data are tracked and logged. Additionally, businesses should ensure that customer data is not modified without customer consent.

Data access control is another important component of the data management framework. Businesses should ensure that customer data is only accessible to authorized personnel, and that access is granted on a need-to-know basis. Additionally, businesses should ensure that customer data is not shared with third parties without customer consent.

Given the importance of data management frameworks for POS credit card processing, it is essential for businesses to ensure that their systems are adequately secured. Vulnerabilities in the POS credit card processing system include unauthorized access, malicious software, data breaches, and data manipulation. To protect against these vulnerabilities, businesses should implement the following security controls:

1. Encryption: Encryption helps to protect customer data from unauthorized access by making data unreadable to anyone without the appropriate key. Businesses should ensure that data is encrypted at rest and in transit to protect customer data from potential threats.

2. Access Control: Access control helps to protect customer data by ensuring that only authorized personnel have access to customer data. Businesses should ensure that access is granted on a need-to-know basis, and that customer data is not shared with third parties without customer consent.

3. Firewalls: Firewalls help to protect customer data from potential threats by blocking malicious traffic and unauthorized access to customer data. Businesses should ensure that their systems are equipped with the latest firewalls to protect customer data.

4. Data Backup: Data backup helps to protect customer data from potential threats by providing a backup of customer data in case of a data breach or system failure. Businesses should ensure that customer data is backed up regularly to ensure that customer data is protected.

Data management frameworks are essential for ensuring the safety and security of customer data associated with point-of-sale credit card processing. Businesses should ensure that their systems are adequately secured in order to protect customer data from potential threats, such as unauthorized access and data breaches. To protect against these threats, businesses should implement security measures, such as encryption, access control, firewalls, and data backup.

# Conclusion

In conclusion, Information Assurance is an important tool for GANT in order to protect the organization’s data from malicious attacks, data breaches, and system failure. GANT should be aware of the vulnerabilities associated with unsecured networks, insecure data storage, and lack of access controls in order to mitigate the risks of data loss, data theft, and data manipulation. Apple Health should take steps to mitigate the risks associated with unauthorized access, data leakage, data manipulation, data loss, and data privacy. Implementing strong authentication measures, encryption protocols, data encryption standards, an audit system, a backup and recovery system, and strict privacy policies and procedures will help to ensure that user data is secure and protected. The payment systems must have adequate security controls in place to protect the data from potential threats and vulnerabilities. Encryption, authentication, access control, and monitoring are all important security controls that should be implemented to ensure the security of the data.

# Recommendations

Data security and privacy is of paramount importance in today’s digital world and organizations need to take steps to ensure their data is secure and protected. For the Group for the Appreciation of the Natterjack Toad (GANT) to ensure their data is secure, they should implement access control, encryption and authentication protocols. For Apple Health, they should implement strong encryption algorithms, authentication protocols, checksums and version control protocols, redundancy and failover protocols, and data storage protocols to protect user data. For payment systems, organizations should implement PCI-DSS compliance, encryption, anti-malware solutions and secure backup solutions to protect customers’ data. These measures will ensure that the organizations’ data is secure and protected from malicious actors and other threats.

# References

Acharya, S., 2020. *What is Information Assurance?..* [Online]   
Available at: https://www.educba.com/what-is-information-assurance/  
[Accessed 10 October 2020].

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

Ataya, G., 2010. *PCI DSS audit and compliance. Information security technical report.* s.l.:s.n.

Bosco, C., 2020. *What is a Data Management Framework?..* [Online]   
Available at: https://www.optimalidm.com/data-management-framework/

Ferrari, A., 2018. *Data Security and Privacy: What You Need to Know..* [Online]   
Available at: https://www.ibm.com/blogs/security/data-security-and-privacy-what-you-need-to-know/

Gorla, S., 2019. *Security Risks That Are Caused By Not Having An Information Assurance System In Place..* [Online]   
Available at: https://www.techfunnel.com/information-security/information-assurance-system-place/  
[Accessed 10 October 2020].

Hu, Z. et al., 2017. *Toward controlled generation of text. In International conference on machine learning.* s.l.:s.n.

Khandelwal, S., 2020. *What Is Data Protection?..* [Online]   
Available at: https://www.investopedia.com/terms/d/data-protection.asp

Kumar, P., Abubakar, M. & Al-Hassan, A., 2020. *Physical Security Challenges and Solutions: A Comprehensive Review..* IEEE Access, 8, 122368-122400. https://doi.org/10.1109/ACCESS.2020.2989369 ed. s.l.:s.n.

Kuo, T. et al., 2017. *Highly oriented Langmuir–Blodgett film of silver cuboctahedra as an effective matrix-free sample plate for surface-as.* s.l.:s.n.

Meer, M., 2020. *What is Data Security? A Comprehensive Guide for Beginners..* [Online]   
Available at: https://www.sophos.com/en-us/medialibrary/PDFs/documentation/sophos-data-security-guide.pdf

Mishra, S., 2020. *Data Accuracy: What It Is & How to Improve It..* [Online]   
Available at: https://www.talend.com/blog/2020/05/21/data-accuracy-what-it-is-how-to-improve-it/

Scherr, M., 2019. *What is Cybersecurity? Everything You Need to Know..* [Online]   
Available at: https://www.csoonline.com/article/3258841/what-is-cybersecurity-everything-you-need-to-know.html

Tuttle, M. & Parise, S., 2017. *Information Security Policies and Procedures: A Practitioner’s Reference..* s.l.:John Wiley & Sons..

# Bibliography

Acharya, S., 2020. *What is Information Assurance?..* [Online]   
Available at: https://www.educba.com/what-is-information-assurance/  
[Accessed 10 October 2020].

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

Ataya, G., 2010. *PCI DSS audit and compliance. Information security technical report.* s.l.:s.n.

Bosco, C., 2020. *What is a Data Management Framework?..* [Online]   
Available at: https://www.optimalidm.com/data-management-framework/

Ferrari, A., 2018. *Data Security and Privacy: What You Need to Know..* [Online]   
Available at: https://www.ibm.com/blogs/security/data-security-and-privacy-what-you-need-to-know/

Gorla, S., 2019. *Security Risks That Are Caused By Not Having An Information Assurance System In Place..* [Online]   
Available at: https://www.techfunnel.com/information-security/information-assurance-system-place/  
[Accessed 10 October 2020].

Hu, Z. et al., 2017. *Toward controlled generation of text. In International conference on machine learning.* s.l.:s.n.

Khandelwal, S., 2020. *What Is Data Protection?..* [Online]   
Available at: https://www.investopedia.com/terms/d/data-protection.asp

Kumar, P., Abubakar, M. & Al-Hassan, A., 2020. *Physical Security Challenges and Solutions: A Comprehensive Review..* IEEE Access, 8, 122368-122400. https://doi.org/10.1109/ACCESS.2020.2989369 ed. s.l.:s.n.

Kuo, T. et al., 2017. *Highly oriented Langmuir–Blodgett film of silver cuboctahedra as an effective matrix-free sample plate for surface-as.* s.l.:s.n.

Meer, M., 2020. *What is Data Security? A Comprehensive Guide for Beginners..* [Online]   
Available at: https://www.sophos.com/en-us/medialibrary/PDFs/documentation/sophos-data-security-guide.pdf

Mishra, S., 2020. *Data Accuracy: What It Is & How to Improve It..* [Online]   
Available at: https://www.talend.com/blog/2020/05/21/data-accuracy-what-it-is-how-to-improve-it/

Scherr, M., 2019. *What is Cybersecurity? Everything You Need to Know..* [Online]   
Available at: https://www.csoonline.com/article/3258841/what-is-cybersecurity-everything-you-need-to-know.html

Tuttle, M. & Parise, S., 2017. *Information Security Policies and Procedures: A Practitioner’s Reference..* s.l.:John Wiley & Sons..