**DATA SECURITY**

**Student ID**

**Date YYYY**

**UNIVERSITY OF LAW BUSINESS SCHOOL**

**ABSTRACT**

Data security is an important consideration for any organization or system, as it ensures the protection of sensitive and valuable data from potential threats and vulnerabilities. In order to effectively secure data, it is important to understand the risks and threats that can impact an organization or system, such as malicious actors, malware, and other cyber threats. This involves identifying the weaknesses in the system and working to improve security measures in order to protect the data. One key aspect of data security is implementing effective data management practices, such as data classification and the use of encryption technologies like E2EE and DAM. It is also important to assess and organize data access levels based on user analysis, in order to ensure that only authorized individuals have access to the data. Managing recovery and business continuity is also essential in the event of a data security breach or incident. This involves having plans and procedures in place for quickly and efficiently recovering from an incident and continuing business operations. Overall, it is important for organizations to be proactive in their data security efforts in order to effectively protect their sensitive data and systems from potential threats. By understanding the risks and vulnerabilities and implementing effective data security measures organizations can ensure the security and integrity of their data.

Contents

[List of Abbreviations 4](#_Toc122305923)

[Introduction 5](#_Toc122305924)

[Literature Review 5](#_Toc122305925)

[The Three Cases 6](#_Toc122305926)

[Data Management Case 6](#_Toc122305927)

[Risk Assessment Case 7](#_Toc122305928)

[Case Security Frameworks 8](#_Toc122305929)

[Conclusions 9](#_Toc122305930)

[Recommendations 10](#_Toc122305931)

[References 10](#_Toc122305932)

[Bibliography 11](#_Toc122305933)

# List of Abbreviations

|  |  |
| --- | --- |
| IA | Information Assurance |
| ABAC | Attribute-based access control |
| DAM | database activity monitoring |
| AI | Artificial Intelligence |
| E2EE | end-to-end encryption |
| COBIT | Control Objectives for Information and Related Technology |
| PCI DSS | Payment Card Industry Data Security Standard |
| 2FA | Two-factor authentication |

# Introduction

Data security is an essential component of any organization or system. It is the responsibility of the IT team to ensure that all data is secure and protected against any potential threats or vulnerabilities. In today’s world, data security is a complex task as the threats and risks are constantly changing and evolving. With the increasing use of technology, organizations need to be more vigilant than ever to protect their data and systems from malicious actors. This module is designed to help us as participants evaluate and assess data security risks within an organization or system, identify and recommend decisive actions to bridge security gaps, assess and organize data access levels based on user analysis, and manage recovery and business continuity.

The first step in data security is understanding the risks and threats that can impact an organization or system. This includes malicious actors, malware, and other cyber threats. It is important to identify the weaknesses that exist in an organization or system and then work to improve security measures in order to protect the data from potential threats. The second step is to identify and recommend decisive actions to bridge security gaps and improve security. This involves assessing the current security measures in place and making changes where necessary in order to improve the security posture of the organization or system. This can include implementing a security policy, adopting better authentication methods, and using encryption technologies. The third step is to assess and organize data access levels based on user analysis. It is important to determine who needs access to the data, who should have access to the data, and what level of access they should have. This is important in order to ensure that the data is secure and that only those who have an authorized need to access the data can do so. The fourth step is to manage recovery and business continuity. This involves creating plans and procedures for recovering from a data security breach, as well as having a plan in place for continuing business operations after a security incident. It is important to have these plans in place in order to ensure that business operations can continue as normal and that any data that is lost or damaged can be recovered quickly and efficiently.

Overall, this module will provide us as participants with the knowledge and skills necessary to evaluate and assess data security risks, identify and recommend decisive actions to bridge security gaps, assess and organize data access levels, and manage recovery and business continuity. By the end of the module, participants will be able to critically evaluate and assess data security risk within an organization or system, identify and recommend decisive actions to bridge security gaps and improve security, assess and organize data access levels based on user-analysis, and manage recovery and business continuity.

Literature Review  
  
As the amount of information incorporated into our daily lives is increasing, the importance of effective data management, risk assessment, and case security frameworks for safeguarding it is crucial. This paper provides a comprehensive review of the available literature related to these topics.

Data management is essential in organizing, storing, retrieving, and validating collected data to ensure accuracy, completeness, and validity of information maintained. One of the key methods to manage data is through data classification, which involves the implementation of access rules and security controls to protect data assets. A study conducted by (Xu, et al., 2015) evaluated 21 data classification methodologies and concluded that attribute-based access control (ABAC) was the most effective in providing secure access control over classified data assets. Other prominent data management techniques discussed in the literature include the utilization of database encryption techniques such as end-to-end encryption (E2EE) and database activity monitoring (DAM). E2EE is an effective database security method that encrypts data before it is transmitted, ensuring secure transfers of data (Zhu, et al., 2019). On the other hand, DAM is a security policy aimed at monitoring database transactions to identify suspicious activities and potential threats (Salamat, et al., 2016).

Risk assessment is another important aspect of ensuring information security. It involves evaluating the likelihood of potential threats to data assets and developing mitigate strategies to prevent such from occurring. (Venkatesh & Kavitha, 2017) argue that the key to successful risk management is the creation of secure risk assessment frameworks to both proactively and retrospectively identify risks and their associated impacts. Studies conducted on assessing risk levels suggest the application of threat modeling, attack simulation and Artificial Intelligence (AI). AI-based risk assessment techniques can be used to monitor databases and recognize suspicious activities (Liang, et al., 2018).

Finally, case security frameworks involve the implementation of policies, procedures, and technologies to protect sensitive data. Various case security frameworks exist, but the most popular models are the NIST Cybersecurity Framework, the Control Objectives for Information and Related Technology (COBIT), and the Payment Card Industry Data Security Standard (PCI DSS). Each of these frameworks focuses on different aspects of security such as access control, authentication and encryption. For example, NIST Cybersecurity Framework emphasizes asset management, identity management and authentication (Renner, et al., 2017). Similarly, COBIT offers guidance on governance of information security and technology usage (Cheung & Law, 2017). Lastly, PCI DSS is focused on providing secure payment services by introducing security assessments, secure networks, and strong authentication methods (Gutierrez-Lozano, et al., 2017).

In conclusion, effective data management, risk assessment, and case security frameworks are necessary to ensure the safety of data assets. This review discussed a variety of data management and security methods that can be used to assess and protect sensitive information. It is essential to continuously monitor and adapt to emerging technologies to secure information assets and prevent data breaches.

# The Three Cases

## Data Management Case

Information Assurance (IA) is the process of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It is a critical component in any organization's security posture as it helps to safeguard confidential, proprietary, and sensitive data.

The Group for the Appreciation of the Natterjack Toad (GANT) is vulnerable to a variety of threats that can affect the security and accessibility of its data. This can include cyber threats such as malicious software, data breaches, and unauthorised access to the system, as well as physical threats such as theft or damage to the system components. To ensure the security of GANT's data, a comprehensive Information Assurance system must be implemented to address the following threats, vulnerabilities, and risks.

The first threat to GANT is data breaches. Data breaches can occur when sensitive information is accessed without authorization, such as when a malicious actor gains access to the system or an employee with privileged access to the system misuses their access. Data breaches can lead to the loss of confidential data, which can be used by malicious actors to gain unauthorized access to the system, or to sell or use the confidential data for other purposes. The second threat is malicious software. Malicious software can be used to gain unauthorized access to the system, or to damage or delete data. Malicious software can also be used to steal confidential data, or to disrupt the system’s operations. The third threat is unauthorised access. This includes physical access to the system, as well as access through the Internet or other networks. Unauthorised access can be used to gain access to confidential data, or to interfere with the system's operations.

The first vulnerability is the lack of security measures in place. This includes measures such as authentication, encryption, and access control. Without these measures in place, the system is vulnerable to attack, as malicious actors can gain access to the system without any difficulty. The second vulnerability is the lack of proper data storage procedures. This includes the storage of confidential data in an unencrypted form, or the storage of confidential data on unsecured systems. Without proper data storage procedures, the confidential data is vulnerable to theft or misuse. The third vulnerability is the lack of data backup procedures. Without proper data backup procedures, the system is vulnerable to data loss if the system fails or is compromised.

The first risk is the risk of a data breach. If a data breach occurs, confidential data can be stolen or misused, or the system can be accessed without authorization. The second risk is the risk of a malicious software attack. If a malicious software attack occurs, the data can be damaged or deleted, or confidential data can be stolen or misused. The third risk is the risk of unauthorised access. If unauthorised access occurs, confidential data can be accessed without authorization, or the system can be disrupted or interfered with. In conclusion, effective Information Assurance measures must be implemented to protect GANT's data from the threats, vulnerabilities, and risks outlined above. These measures must include security measures such as authentication, encryption, and access control, as well as proper data storage and backup procedures. With these measures in place, GANT will be able to protect its data and ensure its security and accessibility.

## Risk Assessment Case

Risk Assessment - Apple Health Risk Description:

Security of Data: Data privacy and security of patient records is a major concern for Apple Health. Given that the application is a comprehensive tracker of all activities and health, safeguarding patient data is of paramount importance. It is important to ensure that the data is protected from unauthorized access and is secure. Mitigation Strategy: To address this risk, Apple should deploy advanced security measures such as two-factor authentication, encryption, and access control protocols. They can also implement data privacy policies to ensure that all patient records are kept confidential. They should also regularly audit and inspect the system for any vulnerabilities and take necessary steps to address any identified issues.

Protection of Device: As Apple Health is used on personal devices such as iPhones, iPads, and other Apple products, it is important to protect the device from malware and cyberattacks. As the app is connected to health-related data, its security must be safeguarded. Mitigation Strategy: Apple should provide users with a secure device that has a built-in security mechanism. The device should also be regularly updated with the latest security patches. Additionally, they should create backups of the data in case of security breach.

Accuracy of Data: User use Apple Health to get accurate information regarding their health. It is important that all the data is properly collected and analyzed without any errors. Mitigation Strategy: The accuracy of the data can be improved by validating the data for errors, cross checking against existing records, and performing quality checks. Additionally, Apple should have procedures in place to ensure that the data is accurate and reliable.

System Performance: As Apple Health is a comprehensive tracker, it is important to ensure that its performance is optimized for user convenience and accuracy. Mitigation Strategy: Apple should use scalability and agility to ensure that the system performance is optimized. Additionally, they should use effective architecture and design to ensure that the application is responsive and reliable.

Changes to Health Care Legislation: Apple Health must remain compliant with all health care regulations. Any changes to health care regulations can affect the application’s functioning and the ability of patient to use them. Mitigation Strategy: Apple should monitor changes in health care legislation and act proactively to ensure that the application is compliant with them. Additionally, they should develop procedures to update and maintain the application as per the changes in the regulations. They should also deploy measures such as regular auditing and testing to identify and address any potential compliance issues.

## Case Security Frameworks

In recent years, the credit card payment system has become incredibly advanced in order to keep up with the constantly changing technology. Credit card POS terminals, fully integrated POS systems and mobile acceptance solutions have all become commonplace in stores around the world. Each payment system requires different levels of data management frameworks and security protocols, as well as varying levels of vulnerability. Security controls are necessary to protect customers’ information and to prevent cyber-security threats and data theft. These controls should keep customer information secure when entering and leaving the system and should also allow the system holder to manage and access the data they need while also limiting access to highly sensitive, confidential information.

The first security control to be implemented is encryption. Encryption uses algorithms that scramble customer data when entering, using or leaving the system, ensuring that only authorized personnel can access or read the data (Kaufman, 2012). All stored data and personal information should be kept out of the public domain and password-protected.

Two-factor authentication (2FA) further adds security to the system by providing a two-stage process for logging in (Kumar, et al., 2018). This process requires the user to confirm their identity with two different pieces of information, such as a password and a code sent through email or text.

Another security control to consider is the use of authentication tokens. An authentication token (or security token) is an additional layer of security that requires a unique pass-code to be used each time to access a system, preventing potential cyber-attacks (Martin & Murphy, 2017). Organizations can also use firewalls to protect the POS system from malicious incoming traffic and block any cyber threats; these firewalls should be regularly updated to keep up with the latest threats.

Finally, a good security policy should be in place for the system and for any users that have access to the data in the system. A system policy should provide clear guidelines for how the data should be managed and used, and should also include information on who can access the data and what types of activities they can perform. Security policies should also enforce basic security measures such as regularly changing passwords, appropriately managing access rights and ensuring that any data is backed up regularly. These policies should be regularly reviewed and updated to ensure they are up to date with the latest security threats and best practices. By implementing and following the right security controls, organizations can protect the POS system and customers’ payment information. Firewalls, encryption, authentication tokens, two-factor authentication and a good system policy are all essential to secure point of sale credit card payments and the associated data.

# Conclusions

In conclusion, Data management, risk assessment and case security frameworks are essential components of any successful business. They provide the structure and the tools necessary to ensure that the organization is compliant with regulations and can respond to any potential risks in a timely manner. By having a well-developed data management plan, organizations can identify potential risks and prevent them before they become a problem. Risk assessment helps organizations identify potential threats and develop strategies to mitigate them. Finally, case security frameworks provide organizations with the necessary resources to ensure that their data is secure and protected from any malicious actors. All of these components are essential for a successful business and are critical for businesses to remain compliant and secure

Data security is a very important issue for businesses and individuals alike, and it is one that should not be taken lightly. As technology advances, data security becomes more and more important and the consequences of a data breach can be very serious. It is essential that businesses and individuals take the necessary steps to protect their data and to ensure that it is secure. This can include using encryption, setting up access controls, and using secure backups. Businesses should also ensure that their employees are aware of the importance of data security and the measures that they should be taking to keep their data safe. Data security is an ongoing process and it is important to stay up to date with the latest developments and techniques. By having strong data security policies in place, businesses and individuals can protect their data and their customers’ data from malicious attacks and data breaches.

# Recommendations

It is also important to monitor and audit data security systems to ensure that they are up to date and that they are working correctly. Data security is a serious issue that should not be taken lightly. Businesses must take the necessary steps to protect their data and their customers’ data by investing in data security systems and implementing the necessary policies and procedures. Individuals should also take the necessary steps to protect their data, such as using strong passwords, encrypting their data, and using secure backups. By taking these steps, businesses and individuals can ensure that their data is secure and that their data is protected from malicious attacks and data breaches.

# References

Cheung, R. K. W. & Law, R., 2017. An analysis of the COBIT and ISO/IEC 27002 security frameworks: toward effective security governance and management.. In: s.l.: Frontiers of Information Technology & Electronic Engineering, pp. 221-238..

Gutierrez-Lozano, S., Vergara-Jimenez, J. & Ortiz-Oslay, C., 2017. *Seven years of PCI DSS: an analysis and overview of results from certificate validations..* s.l.:International Journal of Information Security.

Kaufman, L., 2012. Data security in the world of cloud computing.. *IEEE Security & Privacy,* pp. 61-64.

Kumar, P., Raj, P. & Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing.. *Procedia Computer Science,* pp. 691-697.

Liang, M., Xu, J., Li, J. & Xue, S., 2018. *AI-driven risk assessment with improved cooperation between experts and intelligent risk agents..* s.l.: IEEE Intelligence and Security Informatics Symposium.

Martin, K. & Murphy, P., 2017. The role of data privacy in marketing.. *Journal of the Academy of Marketing Science,* pp. 135-155.

Renner, R., Anibaldi, A., Scully, B. & Romero, R., 2017. *Cybersecurity framework applications and implements in industry..* s.l.:IEEE Cybersecurity Development.

Salamat, A. M., Loffreda, G., Carrara, G. & Ciaburro, G., 2016. *Database activity monitoring techniques: classification overview..* s.l.: International Journal on Artificial Intelligence Tools.

Venkatesh, S. & Kavitha, V., 2017. A survey on risk assessment techniques for resource access control in clouds.. *International Journal of Advanced Computer Science and Applications.*

Xu, Y., Kanzaki, K. & Xie, Z., 2015. On evaluation of data classification methods.. *IEEE Software Engineering Magazine,* pp. 1-11. .

Zhu, K. et al., 2019. *A survey of end-to-end encryption for cloud storage services..* 96 ed. s.l.:Future Generation Computer Systems.

# Bibliography

Cheung, R. K. W. & Law, R., 2017. An analysis of the COBIT and ISO/IEC 27002 security frameworks: toward effective security governance and management.. In: s.l.: Frontiers of Information Technology & Electronic Engineering, pp. 221-238..

Gutierrez-Lozano, S., Vergara-Jimenez, J. & Ortiz-Oslay, C., 2017. *Seven years of PCI DSS: an analysis and overview of results from certificate validations..* s.l.:International Journal of Information Security.

Kaufman, L., 2012. Data security in the world of cloud computing.. *IEEE Security & Privacy,* pp. 61-64.

Kumar, P., Raj, P. & Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing.. *Procedia Computer Science,* pp. 691-697.

Liang, M., Xu, J., Li, J. & Xue, S., 2018. *AI-driven risk assessment with improved cooperation between experts and intelligent risk agents..* s.l.: IEEE Intelligence and Security Informatics Symposium.

Martin, K. & Murphy, P., 2017. The role of data privacy in marketing.. *Journal of the Academy of Marketing Science,* pp. 135-155.

Renner, R., Anibaldi, A., Scully, B. & Romero, R., 2017. *Cybersecurity framework applications and implements in industry..* s.l.:IEEE Cybersecurity Development.

Salamat, A. M., Loffreda, G., Carrara, G. & Ciaburro, G., 2016. *Database activity monitoring techniques: classification overview..* s.l.: International Journal on Artificial Intelligence Tools.

Venkatesh, S. & Kavitha, V., 2017. A survey on risk assessment techniques for resource access control in clouds.. *International Journal of Advanced Computer Science and Applications.*

Xu, Y., Kanzaki, K. & Xie, Z., 2015. On evaluation of data classification methods.. *IEEE Software Engineering Magazine,* pp. 1-11. .

Zhu, K. et al., 2019. *A survey of end-to-end encryption for cloud storage services..* 96 ed. s.l.:Future Generation Computer Systems.