The American University in Cairo
School of Sciences and Engineering

Cyber Security: Case Study

An Assessment of a University Network

CSCE 493002

Selected Topics- Introduction to Cyber Security

Group Members:

Ahmed Emad 900192704

Norhan Al-Atyar 900203525

Roaa Bahaa 900203054

Table of contents

Abstract

In this paper, we investigate the case study of a university in the UK which is transitioning to an online/hybrid learning model. The report evaluates the cybersecurity aspect of the case study and it focuses on the 8 main domains (frameworks) of cyber security which are: Security & Risk Management, Asset Security, Security Architecture & Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Training, Security operations and Software Development Security. It introduces each domain and discusses the strengths and weaknesses of this university in the light of this domain.

1. Security & Risk Management (AHMED EMAD)

1.1. Introduction

In what we're referring to as the fast-changing digital environment , most organizations, including universities, are facing an Expanding scope of threats that varies from cyber threats to physical security threats. This is why it’s more than necessary to implement a comprehensive Security and Risk management system. This section discusses the Security & Risk Management domain.

1.2. Overview

1.2.1. General background

Cybersecurity risk management process of identifying, analysing, evaluating, and addressing cybersecurity threats to protect an organization’s digital assets. This involves both reviewing the existing security measures as well as implementing new solutions to try avoiding or mitigating those risks.

1.2.2. Most relevant sub domains

There is a table in NIST section 2.2 there is a table under the name “SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES” that NIST uses to categorize families and identifiers in the framework published and referenced in this

paper. In this case study which is focusing on the security and risk management of the university campus we are mostly concerned with just a few of them (4 to be exact). Those families are:

1.2.2.1. Access Control (AC)

Risk: Unauthorized access to university's resources, such as student data or academic research, particularly through the central Student Data Management System (SDMS).

Mitigation:

Strong Authentication: Implement multi-factor authentication (MFA) to enhance user access security. This adds an extra verification layer that significantly reduces the potential of having unauthorized users accessing critical systems like the SDMS or specialized computing resources.

Least Privilege Principle: Restrict user access to the minimum necessary for their role. For instance, students should only have view-only access to their grades, preventing unauthorized modifications or unnecessary data exposure.

1.2.2.2. Audit & Accountability (AU)

Risk: Insufficient monitoring of centralized systems, such as SDMS and lecture/tutorial platforms, leading to undetected security incidents or data breaches.

Mitigation:

Robust Auditing Processes: Establish comprehensive auditing for key systems, including the SDMS and academic resources (university researches) . The auditing logs document activities like login attempts, data access by

professors. Regularly examining these logs helps identify anomalous behaviours and potential cybersecurity threats.

Timely Incident Response: Developing response policies to address security incidents swiftly. These policies should outline predefined steps for managing breaches in systems like SDMS, lecture platforms or email resources.

Configuration Management (CM)

Risks: Unauthorized changes to system configurations can introduce vulnerabilities and compromise data integrity, such as altering students' grades or records.

Mitigation:

Authentication Controls: Use multi-factor authentication to ensure only authorized personnel can make changes.

Baseline Configurations: Maintain detailed documentation of all configuration changes, reasons of modifications, individuals involved in the configurations to support auditing.

Validation and Testing: Regularly test and validate configuration changes to confirm they achieve desired outcomes without compromising the data integrity.

Security Assessment and Authorization (CA)

Risk: Insecure software development practices introduce vulnerabilities, as cybersecurity is only as strong as its weakest link, which in this case, is the personnel responsible for software development.

Mitigation:

Continuous Learning: Encourage software developers to stay up-to-date with the latest security trends and emerging threats. Cultivate a culture of continuous learning within the development team to ensure they remain proactive in addressing security challenges.

1.3. A critique of Security and Risk Management analysis done

1.3.1. Pros:

- **Enhancing security posture:** Applying Access Control (AC) ensures that only authorized users are accessing the sensitive information which by its role mitigates the risk of unauthorized access and potential data leaks. Thus boosts the overall security posture (status) of the university.
- **Protection of Student Data:** well configured access controls (AC) can safeguard student data stored in the central Student Data Management System (SDMS).
- **Audit Trail for Accountability**: Audit and Accountability (AU) provides a clear audit trail for user activities. This enhances accountability by enabling the university to monitor and trace actions within critical systems. In the event of security incidents this provides a valuable resource for investigation.

- **Configuration Integrity:** the university can maintain the integrity of system configurations through Configuration Management (CM) which is critical for preventing unauthorized manipulations that could compromise the accuracy of academic records, (exp. students' grades).

1.3.2. Cons:

- **User Experience Challenges:** Students and faculty may find the authentication steps impacting the ease of access to the university's academic resources.
- **Complex Configuration Management:** with the diverse users' requirements the maintainability of the configurations across various systems such as the SDMS and online lecture platforms can be challenging.

1.4. Summary

With an emphasis on four of the main secure control families, this section discusses how the NIST framework might be applied for enhancing the security and risk management on the university campus. It additionally draws attention to some of the dangers in every family and suggests customized mitigating approaches. The review notes certain drawbacks including user experience problems and complexity of configuration management. It also recognizes the advantages, such as improved security posture and student data protection. All things considered, the book offers a thorough summary with practical advice for preserving a safe and resilient academic atmosphere.

2. Asset Security (Ahmed Emad) - Main

2.1. Introduction

"The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes" is how NIST defines an asset or assets. Networks cloud storage, software and apps, on-premise devices, employee and user identification apps, and more can all fall under this category.

2.2. Overview

2.2.1. General Background

The primary goal of asset security in the digital realm is to protect data, hardware, and software resources. The university's move to online education necessitates protecting SDMS, network infrastructure, and student and staff data.

Focus Areas:

- **Data Security:** Protecting information that is stored in the Student Data Management System (SDMS) and the student union (SU) database.
- **Network Security:** Ensuring secure access to the university's network including both on-campus Wi-Fi and remote access for online teaching and learning.
- **Hardware Security:** Securing physical devices such as servers, PCs, and tablets used by staff and students.
- Software Security: Maintaining the integrity of software used for educational and administrative purposes, including the lectures storage software and external systems like the External Plagiarism Checker (EPC).

2.2.2. Suggested Security Policy

The UK university's transition to online teaching necessitates a robust asset management strategy aligned with ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards.

Key components include:

Responsibility for Assets

Inventory of Assets: Maintaining a detailed list of all the hardware and software resources (e.g., computing labs, data center servers) at the university.

Ownership of Assets: Assigning responsibility to individuals like department heads or IT staff for managing specific assets.

Acceptable Use: Defining clear usage policies for devices used in online learning.

Return of Assets: Establishing some protocols for returning the university-issued devices after use.

Information Classification

Guidelines: Categorizing the data by its sensitivity with focusing on student data and academic content.

Labeling and Handling: Implementing labeling systems and secure handling procedures for the classified data.

Media Handling

Removable Media: Develop policies for the secure use of USB drives and similar devices.

Disposal: Ensure secure disposal of sensitive data and media.

Transfer: Establish secure protocols for transferring physical media across campuses.

The policy ensures the security, integrity, and proper management of information assets crucial for the university's digital learning operations.

2.2.3. sample Implementation of the proposed policy

Asset ID	Sensitivity Level	Description	Category	Location	Owner
001	High	SDMS Database	Software	Data Centre	IT Dept.
002	Medium	Lab PCs	Hardware	Shaw Building	Computing Dept.
003	High	Library Network	Network	Smallwood Bldg.	Library
004	Medium	Lecture platform	Software	External Server	Third party

table 2.1

2.3. Critique

2.3.1 Pros

- Efficient Resource Utilization: Optimizes use of hardware and software resources to support online learning.
- Regulatory Compliance: Adheres to ISO/IEC standards, ensuring compliance with data protection laws.
- Enhanced Data Security: Strengthened protection for sensitive student and academic data.

2.3.2 Cons

- Implementation Complexity: Difficult to establish and maintain across diverse departments and campuses.
- · Resource Intensive: Demands significant time, personnel, and financial investment.
- Adaptation Challenges: Staff and students face difficulties adapting to new asset management practices during the online transition.

2.4. Conclusion

The chapter evaluates asset management principles from ISO/IEC 27001:2013 and 27002:2013 within the context of a UK university's shift to online teaching. While the proposed strategy enhances security and compliance, it poses challenges in complexity, resource demands, and adaptation. Moving forward, the university must adopt a robust, adaptable, and balanced approach to ensure secure,

functional, and compliant management of its information assets, safeguarding educational and administrative continuity.

3. Security Architecture & Engineering (Ahmed Emad) - Main

3.1. Introduction

Given that the institution will have several architectures, it is imperative that we address these expectations because we are working with a robust design. Operating systems, networks, and applications are just a few examples of what university architectures might have. Since the university intends to offer its services online to instructors, staff, and students owing to the COVID-19 pandemic, we must dig into security architecture and engineering. While reviewing the standards, controls, and implementation provided by ISO/IEC 27001 and ISO/IEC 27002, we will take a close look at the security architecture and engineering domain.

3.2. Overview

3.2.1. General background

The tools, methods, and procedures you put in place to carry out strong cybersecurity capabilities are referred to as cybersecurity architecture and engineering. Therefore, we must implement a well-engineered architecture to maintain environmental security. As ISO/IEC 27002 demonstrated, any principles for engineering secure systems need to be established, documented, maintained, and applied to any information system implementation efforts.

3.2.2. Implementation guidance

Following the section of ISO/IEC 27002, we will go over the specific guidelines for protecting the development environment, the application services, and the system engineering principles in public networks.

3.2.2.1. For secure application services on public networks.

- the level of confidence each party requires in each other's claimed identity, e.g. through authentication;
- authorization processes associated with who may approve contents of, issue or sign key transactional documents;
- ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;
- determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;
- The level of trust required in the integrity of key documents;
- The protection requirements of any confidential information;

3.2.2.2. For Secure system engineering principles:

- All architecture layers have security built in, striking a balance between accessibility and information security.
- assessing the security risks of each new technology deployment and compare the design to established attack patterns.
- these guidelines and the established engineering practices should be examined on a regular basis.

3.2.2.3. For Secure development environment

- Data sensitivity should be processed, stored, and transmitted by the system.
- Assigning ownership to individuals, like department heads for their respective department assets and IT staff for central systems.
- Security controls already implemented by the organization that supports system development.
- Trustworthiness of personnel working in the environment.

3.3. Critique

3.3.1. Pros

- By offering dependable and secure systems and services to all of its stakeholders, the institution will abide by the law and meet all regulatory obligations in the UK and the EU, such as those outlined in the Data Protection Act, the NIS, or the GDPR.
- Guarantee a more secure, scalable, and robust environment while enhancing the dependability of our systems. This is crucial because it will support the use of both blended and online learning throughout the COVID-19 pandemic.

3.3.2. Cons

The implementation of the secure architecture may present the institution with a number of drawbacks. One problem is that implementing a robust security architecture and engineering requires high complexity, costly price, and resources. It may be expensive, particularly considering the physical size and diversity of the university.

3.4. Summary

Given the COVID-19 epidemic, the Security Architecture and Engineering is crucial and highlights its applicability to our university's plans to offer online services. In accordance with ISO/IEC standards 27001 and 272002, we explore safe system engineering concepts, secure development environments, and protecting application services on public networks. Every aspect's control, guiding principles, and concerns are included in the implementation guidance. Improved security, dependability, scalability, and legal compliance are among its benefits, which increase the university's standing. However, its drawbacks include the intricacy, high implementation costs and resource needs.

4. Communication & Network Security (Roaa Bahaa)

4.1. Introduction

According to ISO/IEC 27002, Communication and network security's main objective is "to ensure the protection of information in networks and its supporting information processing facilities" (ISO/IEC 27002, clause 13.1). This means the information should be safeguarded while being transmitted across the network in terms of confidentiality, integrity and availability. Also, the hardware, such as switches and routers should be protected from both physical threats, such as theft, and cyber threats, such as malwares. Implementing effective management methodology on communication channels and network protocols mitigate the risk of unauthorized access and data breaches which also serves the next domain, Access Management.

4.2. Overview

Communication and Network Security management encompasses having various strategies, policies and technologies protecting the information across the network and the network itself from being intercepted or accessed in a harmful way. This is significant in our case study because for a university to be operating online, those inter-connected sub-networks across the different buildings, such as the Shaw Building and the Reeves Building, must ensure secure data transmission and protection against any potential cyber threats. The main topic I find very relevant to our case study is network segregation. It is simply to divide the network into smaller segments and subnetworks to avoid the risk of any cyberthreat spreading through the whole network which enhances the security. . According to ISO/IEC 27002:2013, Clause 13.1.3, segregating networks reduces the risk of unauthorized access by isolating critical systems from less secure parts of the network (ISO/IEC 27002, clause 13.1).

4.3 Critique

4.3.1 Pros

The first significant pro is that the university follows the idea of network segregation that we have just discussed by having each separate building representing a different sub-network which decreases risk spreading. This is also encouraged by the National Cyber Security Centre (NCSC) in the UK as it makes it harder for the attacker to move from its entry point to its target data (NCSC, 2020).

Second, Pilling Building is the place where critical systems like the central Student Data Management System (SDMS) and corporate email reside, ensuring centralized control and reduced exposure to external threats. The use of this centralized email system also facilitates email monitoring and enables the university to tailor it for its needs and apply the suitable security measurement whether it is an intrusion prevention system or any other measurement.

4.3.2 Cons

Having a campus-wide wifi is definitely efficient to ensure connectivity. However, it introduces a whole new set of risks that needs to be mitigated and avoided. Thus, no clear policies or mechanisms have been mentioned to clarify how the UK university faces such a problem.For example, network scanning tools, Intrusion Detection (IDS) and Prevention Systems (IPS), and end-point protections such as firewalls need to be implemented, as advised by National Institute of Standards and Technology (NIST) (2013, CM-7).

4.4 summary

The Communication and Network Security is the cybersecurity framework that protects both the information travelling across the network and the network hardware as well form any possible threats. This is vital to be ensured in our case study because the university network is a campus-wide wifi, which needs to be protected by policies like encryption, IPS and IDS. However, it was not mentioned how that was done. On the other hand, the university supports network segregation which is one of two key strengths of the case study in this domain. The other one is that the university houses the important services, such as the email system and the SDMS in a separate building.

5. Identity & Access Management (IAM) (Roaa Bahaa)

5.1. Introduction

Identity and Access Management (IAM) is a fundamental domain in cybersecurity as it ensures that data is only accessed by authorized people under specific conditions that include other parameters, such as: the right timing and valid reasons. IAM is needed in all systems, and it is crucial in systems where safeguarding sensitive data is a priority, such as the university case study we are discussing. The fact that the university is also shifting

towards a more hybrid/online learning model makes IAM crucial to ensure seamless data access for all university members without compromising security of data.

5.2. Overview

For any system to implement IAM, it should ensure the following processes are working properly: authentication, authorization and access governance. According to the ISO/IEC 27002, governing these processes should address four key areas: Business Requirements of Access Control, User Access Management, User Responsibilities to protect their authentication information and System and Application Access Control (ISO/IEC, 2013, Clause 9.2). What I believe is most relevant to our case study is Role Based Access Control (RBAC) where depending on your role in the system, you are granted access to specific data. Also, Authentication mechanisms are crucial to choose a secure way to authenticate users, such as Multi-factor authentication (MFA). These two specific topics fall under the umbrella of the first two key areas mentioned and will be closely critiqued in the pros and cons section. Fortunately, cybersecurity laws in the UK (where the university of the case study is located) and many other countries "criminalize unauthorized access to computer systems and data" (UK Government, 2023).

, which acts as a deterrent. However, rather than waiting for such incidents to occur, we must proactively implement measures to detect and prevent these breaches.

5.3. Critique

5.3.1 Pros

We believe the RBAC is well considered in the UK university because as mentioned in the assignment document, an external company is responsible for limiting the access of students to view academic content, while staff can modify it. Also, it was mentioned that the academic staff are authorized to view but not to edit the students information, which is the role of the academic staff. This reflects a very clear segregation of duties which protects data from unauthorized or unintentional modification l (ISO/IEC, 2013, Clause 6.1.2) . It aligns as well with the Least privilege where “every user of the system should operate using the least set of privileges necessary to complete the job” (Schneider, 2003, p. 55).

5.3.2 Cons

Although the IAM seems to be robust and well-implemented in the case study, some gaps were noticed. The first one is that the dormant accounts and how they are dealt with are not mentioned. For example, alumni and retired professors have more restricted access control to data they used to access normally. This should be implemented through an account lifecycle management policy to remove or modify the access rights of such accounts by performing periodic checks on the access rights (ISO/IEC, 2013, Clause 9.2.5). Second, no strong authentication method was mentioned, such as MFA, which might allow unauthorised access to sensitive data. An example of this can be drawn from our university, the American University in Cairo. The careerWeb platform used to have the password of all accounts as the student IDs by default. Thus, a student could access

many careerweb accounts and leak some info, such as student GPAs. Hence, strong authentication methods need to be applied to mitigate such risks.

5.4 Summary

In conclusion, IAM is crucial for ensuring a secure system where data is only accessed by authorized users. This is fundamental while investigating the UK university transition to hybrid learning model. We can conclude that the university applied strong IAM practices, such as RBAC that fulfills both principles of least privilege and segregation of duties. However, gaps remain, including not mentioning how dormant accounts are handled or what strong authentication methods are used to strengthen the IAM framework.

---

6. Security Assessment & Training (Norhan)

6.1 Introduction

As the university adapts to a more online-focused teaching model in response to the COVID-19 pandemic, regular security assessments and comprehensive staff training are crucial for safeguarding online systems from potential threats. This section explores how security assessments and training can be applied to the university's network to enhance its defenses against cyberattacks.

6.2 Review/Overview of Security Assessment & Training

Security assessments help identify vulnerabilities in the university's infrastructure. Various critical systems such as the Student Data Management System (SDMS), email services, and external learning platforms need to be regularly assessed to ensure that they are protected from potential attacks.

For example, the SDMS stores sensitive information such as student details, assignment marks, and progression data. A security assessment should focus on verifying that access controls are robust such that only authorized personnel can modify or view this data. Even less sensitive systems like the plagiarism checker require assessment to protect intellectual property.

In addition to security assessments, staff training is important to reducing human error because it is a common cause of security breaches. Academic staff, administrative staff, and IT professionals all need to understand their role in safeguarding the university's systems. Academic staff need training on recognizing phishing attacks and using secure passwords for systems like the SDMS.

6.3 Critique of Security Assessment & Training

6.3.1 Pros

The most obvious benefit of regular security assessments is that they help identify vulnerabilities before they can be exploited by attackers. Regularly testing can spot weaknesses in these systems and patch them before any damage is done. This is especially important for the SDMS, as it handles sensitive student data, which makes it a prime target for cybercriminals.

Training staff to recognize phishing or use strong passwords reduces data breach risks and ensures compliance with privacy regulations like GDPR, preventing accidental leaks of student data.

6.3.2 Cons

Despite the importance of security assessments, they come with some challenges. Conducting regular penetration tests and vulnerability scans can be time-consuming and costly. Coordinating these assessments across the university's various systems and locations may require significant resources especially with multiple campuses and departments . Additionally, addressing identified vulnerabilities may cause temporary disruptions to services, such as downtime for critical systems like the SDMS or email servers.

Additionally, these assessments may not identify all risks, as new threats and techniques constantly emerge.

Training also has some challenges. Ensuring all university staff are engaged with cybersecurity training can be difficult when users have varying levels of technical expertise. Academic staff, for instance, may need different training than administrative staff, and both may have different levels of understanding about cybersecurity risks.

6.4 Summary

In conclusion, security assessments and training are essential for university online environments. Assessments help identify potential weaknesses and ensure that systems are protected from threats. At the same time, training programs teach staff and students how to spot and avoid common risks. However, universities must be mindful of resource constraints.

---

7. Security Operations (Norhan)

7.1. Introduction

Security operations play a crucial role in ensuring the security and integrity of a university's IT infrastructure. The online learning transition increases cybersecurity risks, such as data breaches and system downtime. Security operations help mitigate these risks by focusing on continuous monitoring, incident management, system availability, and user education. In this section, we explore the importance of these operational components in protecting sensitive data and maintaining secure systems across the university's network.

7.2. Overview

Security operations cover several key functions: continuous monitoring, incident management, system availability, and staff training. According to the National Institute of Standards and Technology (NIST), effective security operations are critical for detecting and responding to threats, maintaining system integrity, and ensuring continuous access to educational resources (NIST, 2013). For the university, which relies on platforms like the Student Data Management System (SDMS) and online learning systems, security operations must focus on safeguarding both academic data and the availability of teaching resources.

- Continuous monitoring is essential to detect security threats in real-time. Using Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems, the university can track unusual activities on its network and respond proactively to potential attacks. For example, unauthorized access attempts to the SDMS can be detected early through these systems (ISO/IEC, 2013). By monitoring network traffic and user behavior, the university can reduce the risk of data breaches and mitigate any damage quickly.

- A well-defined incident response plan (IRP) is essential for responding to security breaches. In the event of a cyberattack or data leak, the IRP outlines steps for containment, investigation, and remediation. The university must ensure that its IRP is tested regularly and that all staff are trained in response procedures (BSI, 2009).
- Ensuring the availability of university systems is crucial for uninterrupted learning. Redundant systems, such as backup servers and load balancing solutions, are used to prevent service disruptions during peak usage periods like registration or submitting exams. The university should also have robust Disaster Recovery Plans (DRPs) to restore services in the event of an attack, like a Distributed Denial of Service (DDoS) attack. These measures ensure that essential systems remain accessible (ISO/IEC, 2013).

7.3. Critique

7.3.1 Pros

The university's security operations framework has several strengths. Continuous monitoring helps detect threats early. Incident response plan allows for quick mitigation. System availability is maintained through redundancy and disaster recovery plans that ensures online resources remain accessible (BSI, 2009).

7.3.2 Cons

However, there are challenges in maintaining these security operations. The cost and resources required for continuous monitoring and maintaining a 24/7 incident response capability are significant. Additionally, ensuring the availability of systems during periods of high demand, particularly in a hybrid learning model, can be complex and resource-intensive. (ISO/IEC, 2013).

7.4. Summary

In conclusion, security operations are essential for maintaining the security and availability of the university's systems as it transitions to a more online-focused environment. Continuous monitoring, incident management and system availability are key components of this security framework.

8. Software Development security (Norhan)

8.1. Introduction

Systems like the Student Data Management System (SDMS), Learning Management System (LMS), and email system are vital to the university's operations which makes them targets for cyber threats. Implementing strong security throughout the software development lifecycle (SDLC) is necessary to protect these systems.

8.2. Overview

Software development security involves integrating security throughout design, development, and deployment. Key elements, as per ISO/IEC 27002, include **secure coding standards**, **code reviews**, **vulnerability scanning**, and **penetration testing** (ISO/IEC, 2013, Clause 14.2).

The following security practices are essential to follow:

- Secure Design by embedding encryption and secure authentication mechanisms.
- Regularly reviewing code for vulnerabilities.
- Automated vulnerability scanning to detect weaknesses.
- Identifying and fixing flaws before deployment.

- Testing for security issues during development.

For example, **role-based access control (RBAC)** in the SDMS ensures that academic staff can view, but not modify, student data, while administrative staff have modification privileges. This ensures only authorized personnel access sensitive data.

8.3. Critique

8.3.1 Pros

The university has effectively implemented Role-Based Access Control (RBAC) in the Student Data Management System (SDMS) that ensures that users only have access to the data necessary for their role. For example, academic staff can view student information, but they cannot modify it.

Additionally, the centralized email system helps to mitigate phishing risks by managing user access from a single point, which makes it easier to monitor and secure communications. The separation of the Students Union (SU) system from the SDMS adds an extra layer of protection. This ensures that data in the two systems cannot be accessed or tampered with by unauthorized users or systems.

Lastly, the use of external vendors to manage the Learning Management System (LMS) means that the university can leverage the vendor's expertise and security measures which reduces the university's direct responsibility for the security of the system while ensuring that professional security protocols are in place.

8.3.2 Cons

There are areas for improvement, such as the lack of regular security testing for internally developed systems. Without frequent testing, vulnerabilities may go undetected. Additionally, the management of third-party software dependencies needs attention, as outdated or insecure libraries can pose risks. The code review process could also be improved by emphasizing security to identify and fix potential flaws before deployment.

8.3.3 Recommendations

The university should:

- Perform regular security testing, including penetration testing, on all internal systems.
- Implement a dependency management policy to ensure third-party software is up to date and secure.
- Strengthen the code review process with a focus on secure coding practices.
- Integrate security into the CI/CD pipeline, automating security checks during development.

8.4. Summary

Software development security is crucial to protecting the university’s sensitive data. The university has implemented important security practices, such as RBAC in the SDMS and external vendors for the LMS. However, there are gaps, including the need for more frequent security testing and better management of third-party software. Addressing these issues will strengthen the university's security.

References

BS ISO/IEC 27002:2013 (2013) *Information Technology — Security Techniques — Code of Practice for Information Security Controls*. Geneva: ISO/IEC.

British Standards Institution (BSI). (2009) *BS ISO/IEC 27004: Information Technology — Security Techniques — Information Security Management Measurements*. London: BSI.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2013) *ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls*. Geneva: ISO/IEC.

National Institute of Standards and Technology (NIST). (2013) NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, MD: U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.800-53r4.

NCSC. (2020) Preventing lateral movement. [online] Available at: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement[Accessed 8 December 2024].

Schneider, F.B. (2003) 'Least privilege and more [computer security]', *IEEE Security & Privacy*, 1(5), pp. 55–59. doi: 10.1109/MSECP.2003.1236236.

UK Government. (2023) Review of the Computer Misuse Act 1990: Consultation and response to call for information. Available at: https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible