Cyber Security Case Study Report

CSCE 3423 - Introduction to Cyber Security

Adham Salem, Toqa Mahmoud, Merna Hebishy, Ismail Sabry

May 20, 2025

Abstract

This report delivers a detailed cybersecurity case study conducted for a fictional UK university that has recently transitioned to online and blended learning models. The assessment is structured around the eight domains of cybersecurity as defined by globally recognized standards such as NIST and ISO/IEC 27001. It identifies critical security risks, evaluates the institution's current security posture, and provides a set of actionable recommendations. Emphasis is placed on enhancing governance, protecting digital and physical assets, securing communications, and promoting a culture of cyber awareness across staff and students. The objective is to support the university's efforts in ensuring confidentiality, integrity, and availability of its information systems.

Contents

1. Security & Risk Management

1.1. Introduction

Security and Risk Management is a critical area within cybersecurity that involves identifying, evaluating, and managing potential risks that could harm the university's information and technology assets. With the increasing reliance on online learning platforms and digital infrastructure, comprehensive risk management practices are vital to maintain the confidentiality, integrity, and availability of critical data and services.

1.2. Review/Overview

The university operates over multiple campuses: the Main Campus (hosting departments such as Computing, Business, Life Sciences, Law, and Arts), the Health Campus situated 20 miles away, and the London Campus specialized in computing courses. Each campus presents unique cybersecurity risks due to their varied locations and functions.

Key systems include:

- **Student Data Management System**, which holds sensitive information such as student details and academic records.
- **Email and Web Servers** that manage internal and external communications.
- **Student Union System**, isolated from the main data system, manages student inquiries and interactions as well as society membership and management.
- **External Lecture Management System** integrated with a plagiarism checker, hosting tutorials and lecture materials.

1.3. Detailed Risk Identification and Analysis

Risks in cybersecurity are assessed based on threats, vulnerabilities, and the potential impacts they may cause. Below, we comprehensively review the identified risks.

Asset	Threat	Vulnerability	Impact	Likelihood	Risk Level
Student Data Management System	Unauthorized access, data breaches	Weak passwords, inadequate role-based access controls	Very High	High	Critical
Email and Web Servers	Phishing and Malware attacks	Insufficient security software, lack of staff training	High	Medium	High
Student Union System	Malware infection, unauthorized access	Outdated security protocols, poor network segregation	Medium	High	High

Lecture Management System	Intellectual property theft, unauthorized modifications	Third-party dependency, weak contractual security requirements	Very High	Medium	High
Campus Wi-Fi Networks	Unauthorized network access, data interception	Weak encryption standards, insufficient network monitoring	High	Medium	High
Staff Surface Pros	Device theft, sensitive data leakage	Lack of mandatory encryption, poor physical security measures	Very High	High	Critical

1.4. Recommended Risk Treatment Strategies

Risk treatment strategies involve specific measures aimed at reducing identified risks. Below are comprehensive recommendations explained:

- Enhance role-based access controls and enforce strong password policies for the Student Data Management System. Regularly audit and monitor access logs.
- Implement advanced anti-malware software and conduct ongoing cybersecurity awareness training to reduce the impact of phishing and malware.
- Upgrade the Student Union System's servers, applying Endpoint Detection and Response solutions to promptly detect and mitigate malware infections.
- Negotiate comprehensive security agreements with external service providers, mandating regular independent security audits and compliance with international standards.
- Strengthen network security across all campuses by deploying robust firewalls, encryption protocols, and continuous monitoring systems.
- Mandate full-disk encryption and device tracking for all portable devices issued to staff.

1.5. Critique

Pros:

- **Institution-wide risk visibility:** The assessment identifies risks across all departments and campuses — from the centrally located Student Data Management System in the Pilling Building to the isolated Student Union server in the Reeves Building.
- **Protection of sensitive data and infrastructure:** By addressing threats to academic records, student personal data, and intellectual property, the university

can enforce protective measures across physical devices, servers, and third-party systems.

- **Alignment with recognized security frameworks:** Mapping recommendations to established standards like ISO/IEC 27001 provides structure, credibility, and a clear path to compliance with legal requirements such as the United Kingdom's Data Protection Act.
- **Improved incident response readiness:** A structured security strategy enables the university to prepare for, detect, and respond to cyber threats in a timely and coordinated manner.

Cons:

- **Operational and resource burden:** Effective implementation of risk management practices requires sustained investment in tools, personnel, and training across multiple geographically dispersed locations.
- **Decentralized infrastructure complexity:** The diverse nature of systems — from on-campus lab equipment to externally managed lecture platforms — complicates consistent enforcement of controls and increases the likelihood of gaps.
- **Limited control over third-party services:** Reliance on external providers for core systems (e.g., the lecture management system and plagiarism checker) introduces risks that cannot be fully mitigated internally.

1.6. Summary

Security and Risk Management plays a central role in defending the university's academic mission in a digital age. This domain provides a systematic approach to identifying, evaluating, and addressing threats to student data, institutional knowledge, and core services. By applying international security standards and aligning them with the university's actual infrastructure — including its departmental subnets, remote campuses, and cloud integrations — the institution strengthens its resilience against disruptions and data loss.

2. Asset Security

2.1. Introduction

Asset Security refers to the systematic protection of physical and digital resources that hold value to the university. These assets include data, systems, equipment, and intellectual property. With an increasing dependency on distributed computing environments, cloud services, and mobile access, it is essential to implement structured, risk-based controls to protect university assets throughout their entire lifecycle—from creation to disposal. In this section, we will explore how university assets are identified and classified, the controls used to protect them, how assets are managed throughout their lifecycle, specific case vulnerabilities, and the strengths and weaknesses of the current asset security approach.

2.2. Asset Identification and Classification

To manage security effectively, all assets must be first identified, categorized, and classified based on their sensitivity and importance.

- **Information assets:** Student records, staff files, academic transcripts, and research data.
- **Hardware assets:** Surface Pro tablets used by staff, desktop computers in computing labs (Shaw Building), servers housed in Pilling and Reeves Buildings.
- **Software assets:** Student Data Management System (SDMS), Email and Web Services, Plagiarism Checker, Lecture Content Platform.
- **Network assets:** Subnet routers, firewalls, wireless access points across all buildings.
- **Human assets:** Academic staff, IT administrators, student union representatives, and contractors.

Classification should be done using a three-tier structure:

- **Public:** Intended for open dissemination (e.g., university course descriptions).
- **Internal Use Only:** For access by authorized university members (e.g., staff memos, timetables).
- **Confidential:** Highly sensitive data that, if breached, would cause significant harm (e.g., student marks, personal details, proprietary research).

2.3. Review/Overview

Asset protection must be implemented through policy enforcement, technical controls, and administrative safeguards.

2.3.1. Information Assets

- Encrypt all sensitive data at rest and in transit using industry-standard encryption.

- Store confidential data (such as student academic history) only in secure, access-controlled environments like SDMS.
- Apply role-based access controls and regularly audit access logs.

2.3.2. Hardware Assets

- Maintain a full inventory of university-issued laptops and Surface Pros.
- Ensure all portable devices have enforced full-disk encryption and automatic lock screens.
- Label devices with asset tags and associate them with individual users for accountability.
- Use cable locks, locked storage cabinets, and access-controlled offices to prevent theft.

2.3.3. Software Assets

- Install only licensed, approved software on lab PCs and staff computers.
- Secure administrative tools such as SDMS and plagiarism systems with multi-factor authentication.
- Regularly patch software and decommission outdated or unmaintained platforms.

2.3.4. Network Assets

- Apply strict segmentation across building subnets to prevent lateral movement between departments.
- Configure Wi-Fi with enterprise-level encryption (e.g., WPA3-Enterprise) and RADIUS-based authentication.
- Use firewalls and intrusion detection systems (IDS) at network gateways.
- Monitor network traffic for anomalies and unauthorized data transfers.

2.3.5. Human Assets

- Conduct regular training on data handling, phishing recognition, and device security.
- Establish clear acceptable use policies for all staff and students.
- Limit privileges for external vendors and contractors.

2.4. Asset Lifecycle Management

Each asset must be protected at every stage of its lifecycle. The lifecycle includes the following five distinct phases:

- **Acquisition:** Before any hardware or software enters the university environment, it should be verified against security procurement policies. This includes sourcing hardware from trusted vendors, verifying the absence of supply chain compromises, and validating software licenses to ensure legal and secure installation.

- **Deployment:** Assets must be configured securely. This involves disabling unused services, installing endpoint protection, assigning ownership, and applying baseline security configurations. Systems should be deployed based on the principle of least privilege.
- **Usage:** While assets are active, continuous monitoring and user policy enforcement are essential. This includes preventing data misuse, applying access controls, logging all interactions with sensitive data, and educating users on proper usage and security protocols.
- **Maintenance:** During active use, assets should receive timely security updates, be included in patch management cycles, and undergo routine configuration reviews. Vulnerability assessments should also be performed to uncover misconfigurations or weaknesses.
- **Decommissioning:** Assets that are no longer needed must be securely removed from service. This means performing certified data destruction on storage media (e.g., using NIST SP 800-88 standards), wiping user profiles, revoking access credentials, and updating the asset registry to reflect the status change.

2.5. Case-Specific Scenarios and Vulnerabilities

- **Reeves Building – SU Server:** Not integrated with SDMS; risk of weak encryption and physical exposure.
- **Surface Pros:** Often carried off-site; potential for loss or theft without remote wipe or tracking features.
- **Lecture Platform and EPC:** Managed by third party overseas; lack of control over data residency and user access.
- **Wi-Fi Across Subnets:** Without proper isolation, a compromised lab machine in Shaw could be used to pivot into administrative systems in Davenport.

2.6. Critique

Pros:

- **Full lifecycle coverage:** The university's asset management plan incorporates protection from acquisition to decommissioning, ensuring assets do not fall through gaps in policy.
- **Cross-domain applicability:** Policies designed for hardware and software extend to cloud platforms and remote access devices, which are essential in the context of digital learning.
- **Legal and regulatory alignment:** By integrating ISO/IEC 27002 controls and complying with GDPR requirements, the university avoids legal pitfalls and protects the privacy of students and staff.

Cons:

- **Asset sprawl:** The university's multi-building and multi-campus structure makes centralized inventory control difficult. Devices like staff-issued Surface Pros may escape notice or remain improperly secured.
- **Human oversight:** Staff may fail to apply asset handling protocols correctly due to lack of training or awareness. This is especially risky in environments where BYOD (Bring Your Own Device) is informally permitted.
- **Third-party risks:** Data stored on the cloud-hosted lecture platform or accessed by the external plagiarism checker cannot be fully monitored or controlled by internal security teams.

2.7. Summary

Asset security at the university must evolve to address a diverse and rapidly changing digital environment. It is not sufficient to manage only traditional hardware or internal data centers. Security protocols must span the entire lifecycle of digital and physical assets and extend to cloud applications, third-party tools, and remote access devices. Effective implementation requires collaboration between IT administrators, academic staff, external vendors, and policy makers to maintain a unified and secure operational ecosystem.

3. Security Architecture & Engineering

3.1. Introduction

Security architecture and engineering provide the structural and procedural safeguards that ensure the confidentiality, integrity, and availability of information systems. In the wake of COVID-19, our UK university has accelerated its adoption of online and blended learning. This shift demands a reassessment of how securely its diverse digital assets—student data, teaching materials, and support services—are designed, deployed, and maintained. Guided primarily by *ISO/IEC27002:2013* and complementary standards (e.g. NISTSP 800-160), this section introduces the scope, objectives, and context of a modern security architecture for the institution.

3.2. Review/Overview

3.2.1. General Background

Security architecture establishes the high-level design principles that govern networks, applications, data flows, and physical assets. Security engineering applies those principles—via hardening, segmentation, cryptography, and assurance testing—to build and operate trustworthy systems.

The university hosts six academic departments on a main campus, one remote health campus, and a specialist London centre. Core services include:

- a centralised Student Data Management System (SDMS) in the on premise data centre;
- a university e-mail platform and public web server, also on premise;
- a cloud-hosted learning content system with links to an external plagiarism checker (EPC);
- an autonomous Students' Union (SU) server in a non-data-centre building (Reeves);
- ten specialised computing labs, widespread Wi-Fi, and subnetted building networks.

3.2.2. Key Technical Topics

1) **Secure System Engineering Principles**—per ISO/IEC27002§4.2.5, security must be embedded across business, data, application, and technology layers. Threat modelling and secure coding checkpoints are mandated in every project milestone.
2) **Defense-in-Depth**—firewalls, network ACLs, and a campus Security Information and Event Management (SIEM) platform limit lateral movement and provide real-time telemetry.
3) **Segmentation and Isolation**—each building is a routed subnet; critical services such as SDMS reside in dedicated VLANs with strict RBAC.
4) **Endpoint Security**—Enterprise Mobility Management (EMM) and Endpoint Detection and Response (EDR) protect staff PCs and Surface Pros; configuration baselines follow the UK NCSC Cyber Essentials scheme.

5) **Secure Software Development Lifecycle (SSDLC)**—static/dynamic analysis, dependency scanning, and signed releases are integrated into the CI/CD pipeline.

6) **Cloud Security and Data Residency**—contracts for the out-of-UK content repository and EPC mandate AES-256 at rest, TLS 1.3 in transit, and GDPR-compliant processing clauses.

3.3. Critique

3.3.1. Pros

- **Centralised Data Management** in SDMS fosters uniform access control and simplifies GDPR auditing.
- **Network Segregation** by building constrains breach blast-radius, supporting Zero-Trust micro-segmentation strategies.
- **Scalable Cloud Services** provide elasticity and robust disaster-recovery capabilities for lecture delivery.
- **Remote-Access Enablement** via VPN and federated SSO sustains teaching continuity across dispersed campuses.

3.3.2. Cons

- **Legacy & Shadow IT**—departmental data silos and the SU server may bypass central policies, exposing unpatched services.
- **Data Residency Risks**—storing academic IP in non-UK data centres complicates contractual and regulatory compliance.
- **Fragmented Identity Management**—the absence of a unified IAM platform causes privilege creep and delayed off-boarding.
- **BYOD / Endpoint Diversity**—heterogeneous devices increase the attack surface and strain patch-management processes.
- **Physical Security Gaps**—servers located outside the main data centre lack redundant power, environmental controls, and monitored access.

3.4. Summary

The university's transition to online teaching accentuates both the value and fragility of its digital estate. Strengths include a central SDMS, well-defined subnet architecture, and emerging cloud capabilities. Weaknesses lie in inconsistent identity governance, endpoint hygiene, and jurisdictional data-protection challenges. By adopting a unified IAM solution, extending Zero-Trust segmentation, and rigorously applying SSDLC practices, the university can align its security posture with sector best practice while enabling innovative learning modes.

4. Communication & Network Security

4.1. Introduction

In today's digitally connected academic environments, securing communication channels and network infrastructure is essential to maintaining the confidentiality, integrity, and availability of institutional data. As the university shifts toward a more online and distributed teaching model, communication and network security becomes a critical domain within its broader cybersecurity strategy. This section explores the purpose and significance of communication and network security, examines the university's current infrastructure in light of ISO/IEC 27002:2013 best practices, and provides a critique highlighting both the benefits and challenges of implementing robust network security measuress.

4.2. Review/Overview

The university operates a complex and distributed network environment. It includes multiple geographically separated campuses such as a Health department located 20 miles from the main campus and a sub-campus in London — all of which are connected to the main university network. Each building is designated as a subnet, suggesting a degree of logical segmentation within the infrastructure.

Wi-Fi is accessible throughout the campus, but there is no information on the type of security controls implemented to protect wireless communication. This lack of detail raises concerns regarding potential vulnerabilities, such as unauthorized access or data interception, especially in high-traffic or public areas.

Several critical systems are integrated into the university's infrastructure. The central Student Data Management System (SDMS) is accessible by all employees, with access controlled by role and grade. In addition, the university website and the Student Union's internal system manage essential student-facing services, while academic content is handled by a third-party platform hosted outside the UK and linked to an external plagiarism checker (EPC). These dependencies on internal and external systems highlight the importance of securing both internal data traffic and communication with cloud-based services.

No mention of the use of encrypted tunnels (e.g., VPN) for inter-campus communication, nor does it clarify whether there are restrictions between subnets. Similarly, there is no indication of formal agreements or security reviews related to the EPC platform. These omissions suggest gaps in communication and network security practices, particularly in areas aligned with ISO/IEC 27002:2013 Clause 13, including network segregation (13.1.3), data protection in transit (13.1.1), and secure external data exchange (13.2.2).

Overall, while the university's infrastructure is logically structured and centralized, it lacks visible enforcement of key communication and network security measures. Addressing these gaps is essential to ensure data confidentiality, integrity, and resilience across its interconnected systems.

4.3. Critique

This section provides a critical evaluation of communication and network security as it applies to the university's infrastructure. Drawing on ISO/IEC 27002 controls and the specific conditions outlined in the University's case, the critique explores both the advantages and challenges of implementing effective network security measures. While these controls can significantly enhance the confidentiality, integrity, and availability of university systems, they may also introduce complexity, cost, or operational constraints.

4.3.1. Pros

Implementing communication and network security brings several advantages to the university:

- **Reduced Risk of Data Breach Across Subnets:** Implementing controls from ISO 27002:13.1.3(network segregation) ensures that each building and department, which are already subnetted, can be better isolated. For example, segmenting the SU's system in the Reeves Building from the SMDS (Student Management Data System) in the Pilling Building reduces the blast radius of a breach; if a threat actor compromises a system in the SU (Student Union) subnet, proper network segregation would prevent lateral movement to more sensitive systmes like the SDMS.
- **Clear Accountability via Logging and Monitoring:** Controls under ISO 27002:13.1.1(d) recommend detailed logging. Implementing centralized log management for network traffic supports both incident response and digital forensics. For instance, if a DDoS attack targets the university website, historical logs can help trace the source of the attack, supporting both recovery actions and legal investigations.
- **Improved Control of External Connections and Cloud Usage:** ISO/IEC 27002 emphasizes the importance of establishing secure information transfer agreements with external parties (Clause 13.2.2). The university states that "There is a link to an External Plagiarism Checker – EPC – hosted on the cloud," and that "the data centre for this system is located outside of the UK and is held in a secure site." While the security posture of the EPC system is not detailed, such external dependencies necessitate formal agreements that define security responsibilities. These agreements — typically in the form of Service Level Agreements (SLAs) — should cover encryption standards, data availability, incident handling, and liability. In the event of a breach, a well-structured agreement ensures that the university can trace accountability, enforce contractual obligations, and protect academic integrity.
- **Alignment with International Standards and Improved Reputation:** Following internationally recognized standards such as ISO/IEC 27002 can contribute to the university's reputation for strong information security. This may enhance trust among students, staff, and external stakeholders, and potentially support research funding applications or collaborative partnerships, as seen in other institutions that emphasize ISO compliance in their strategic planning.
- **Increased Resilience and Fault Isolation:** Segmenting the university's network by building and department not only improves security, but also helps contain faults and minimize downtime. If one subnet (e.g., in the Reeves Building) experiences a

network failure or cyberattack, it can be isolated without affecting the core systems in the Pilling Building or other departments, thus preserving business continuity.

- **Enforcement of Role-Based Access at Network Level:** ISO13.1.1(g) and 13.2.3 suggest network-level access restrictions and strong authentication. By integrating network security with identity and access management controls, the university can enforce access policies at multiple layers, including application, system, and network. For example, student and academic roles that have different access rights to the online content platform can be further secured with network-based access control mechanisms, reducing the risk of privilege misuse.
- **Secure Connectivity Between Distributed Campuses:** As the university spans multiple physical locations, including a remote Health department and a London sub-campus, communication and network security controls such as VPNs and encrypted tunnels are essential to maintaining secure inter-campus data exchange. These controls ensure that sensitive academic or administrative information remains protected even when transmitted over untrusted networks. This alligns with ISO 13.1.1(c) and 13.1.2: Protecting data over public networks and Ensuring secure service levels.

4.3.2. Cons

Although communication and network security controls offer significant protection and operational benefits, their implementation is not without challenges.

- **High Implementation and Maintenance Cost:** Deploying advanced network segmentation, VPNs, and full-time monitoring requires substantial investments in hardware(firewalls, managed switches) and skilled staff. Segregating each department with firewalls and VLANs would require configuration, training, and frequent audits, adding ongoing financial and resource costs.
- **Operational Complexity and Delays:** Strong controls such as as encryptions, gateway filtering, and strict access rules may slow down everyday operations, particularly for academic content sharing or IT support tasks. For example, a lecturer trying to quickly upload material to a lecture server hosted offsite might face authentication barriers , creating frustration and time loss
- **Potential for Misconfiguration and False Sense of Security:** Complex network controls, if not configured correctly (e.g., firewall rules or VPNs), can create vulnerabilities or block critical academic services. If the SDMS is unintentionally restricted iced by ACLs from the Health campus for example, it might disrupt grading workflows for staff 20 miles away, affecting operations.
- **Increased Burden on Non-Technical Staff:** ISO complaint communication policies (check ISO 27002:13.2.1/13.2.3) requires staff to follow strict procedures for email, file transfer, and messaging. Non-IT users may find these inconvenient or confusing, a staff my resort to personal email or file-sharing services if university systems are too complex, introducing shadow IT risks.
- **Overdependence on External Providers and Legal Risks:** The plagiarism checker is managed by an external cloud provider. Without robust agreements (ISO

27002:13.2.2), the university is exposed to service outages or breaches it cannot fully control. If the EPC could disrupt academic timelines and damage credibility.

- **No Mention of Network Access Control for Devices :** No information is given about verifying or restricting which devices connect to the network (e.g., BYOD, staff Surface Pros, lab machines).Any unauthorized or infected device could connect to the Wi-Fi or internal network, potentially compromising other systems, ISO 13.1.1 (f, g), Systems on the network should be authenticated and network access should be restricted, needs to be implemented.

- **No Mention of Encryption for Data in Transit:** SDMS is accessed by multiple users across departments and campuses, but there's no mention of encrypted communication (e.g., HTTPS, VPNs). Data such as student records or academic files could be intercepted during transmission, especially from remote campuses or via Wi-Fi. ISO 13.1.1 (c) 13.2.1 (a, f), Data passing over public/wireless networks should be encrypted, should be added into consideration.

- **No Formal Policies for Information Transfer or Messaging:** There's no mention of staff or student policies for how to share documents, use email securely, or handle attachments.Users may unknowingly send sensitive data over insecure channels (e.g., personal Gmail, unencrypted USBs), leading to data leaks or malware infections. ISO 13.2.1 13.2.3, Formal policies should guide secure communication (email, messaging, file transfer), can be adapted.

- **Unclear if Any Agreements Exist for Cloud Services:** EPC (external plagiarism system) is hosted offsite, but no detail is given about formal SLAs or data protection agreements. In case of a breach, the university may have no recourse or enforcement capability without a contract defining liability and security terms. ISO 13.2.2, Secure information transfer agreements should be in place with external parties, must be implemented.

4.4. Summary

Communication and network security is a fundamental pillar of a secure academic IT infrastructure, particularly in the context of a modern, digitally connected university. This section reviewed the domain through the lens of ISO/IEC 27002:2013, highlighting essential controls such as network segmentation, secure wireless access, encrypted data transmission, access control, and monitoring.

Through analysis of the university, several strengths and vulnerabilities were identified. On the positive side, a subnetted network design, centralized systems, and potential for aligning with international standards position the university well for adopting robust network security practices. However, the lack of explicit mention of key security implementations—such as secure Wi-Fi protocols, logging systems, encryption of data in transit, and secure agreements with external service providers—presents critical areas of concern.

The critique outlined both the advantages and drawbacks of implementing communication and network security controls. While such measures improve resilience, accountability, and compliance, they may also introduce cost, complexity, and usability challenges.

5. Identity & Access Management

5.1. Introduction

Identity and Access Management (IAM) is the discipline that ensures the right individuals gain the right level of access to the right resources at the right time. For a multi-campus UK university embracing blended learning, robust IAM underpins both security and usability, safeguarding sensitive student data while supporting seamless collaboration across departments, campuses, and cloud platforms.

5.2. Review/Overview

5.2.1. General Background

IAM spans the life-cycle of digital identities—from initial onboarding through periodic entitlement reviews to final de-provisioning. Modern IAM platforms integrate authentication, authorisation, and accounting, enabling single sign-on (SSO) experiences, granular role-based controls, and comprehensive audit trails.

5.2.2. Key Technical Topics

- *Federated Identity Management*—enables cross-domain authentication between on-premise systems (e-mail, SDMS) and cloud services (learning content platform, EPC) via SAML 2.0 or OpenID Connect.
- *Role-Based Access Control (RBAC)*—links entitlements to job roles and grades, mirroring university governance structures and facilitating least-privilege enforcement.
- *Multi-Factor Authentication (MFA)*—introduces an additional verification layer for privileged or remote access, mitigating credential-theft risks.
- *Lifecycle Management and Provisioning*—automates account creation, modification, and removal as students enrol, progress, graduate, or staff change roles.
- *Privileged Access Management (PAM)*—vaults and monitors high-risk administrative accounts, limiting exposure of domain controllers, database servers, and network devices.
- *Logging and Monitoring*—centralises authentication logs, enabling anomaly detection and rapid incident response.

5.3. Critique

5.3.1. Pros

- Streamlines user experience via single sign-on while maintaining isolated data domains between departments and campuses.
- Enforces least-privilege principles, reducing accidental or malicious data exposure—especially critical for SDMS records.

- Simplifies regulatory compliance efforts (e.g. GDPR) through consistent access governance and auditable entitlements.
- Provides stronger defences against phishing and credential stuffing by mandating MFA for high-value resources.

5.3.2. Cons

- Architectural complexity rises when integrating legacy on-premise solutions with modern cloud platforms and external partners.
- Performance or usability may suffer if authentication flows introduce latency or require frequent re-authentication.
- Up-front costs for licensing, deployment, and staff training can be significant—especially when extended to specialised labs.
- Continuous governance overhead: entitlements must be reviewed regularly, and dormant or orphaned accounts promptly disabled.

5.4. Summary

A comprehensive IAM framework—combining federated identity, RBAC, MFA, and automated lifecycle management—provides the foundation for secure, user-friendly access across the university's distributed infrastructure. Although implementation entails financial and operational challenges, robust IAM significantly mitigates data-breach risks, enhances compliance posture, and supports the flexible learning ecosystem demanded in a post-COVID environment.

6. Security Assessment & Training

6.1. Introduction

Security assessment and training are essential for a comprehensive information security management framework. Regular assessments help organizations identify vulnerabilities, test defenses, and ensure systems remain compliant with security standards. Training and awareness programs equip users with the knowledge and vigilance required to recognize and respond to cyber threats.

In the case of the university, these functions are particularly critical. The institution operates a centralized Student Data Management System (SDMS), uses cloud-based tools like the External Plagiarism Checker (EPC), and grants system access to a wide range of academic and administrative users across multiple campuses. This distributed and digitally integrated environment demands a proactive approach to technical security assessments and user awareness.

This section evaluates how the university currently addresses security assessment and training, identifies observed strengths and gaps based on the university, and relates these findings to best practices outlined in the ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 series of standards.

6.2. Review/Overview

The domain of security assessment and training consists of two interrelated components. First, security assessments, such as vulnerability scans, penetration testing, and compliance audits, are designed to evaluate the effectiveness of security controls and identify areas of risk. ISO/IEC 27002:2013 (Clause 18.2.1–18.2.3) emphasizes the need for regular reviews of technical systems and processes, while ISO/IEC 27004 provides metrics to measure their impact.

Second, training and awareness initiatives ensure that employees, students, and stakeholders understand their security responsibilities. ISO/IEC 27002 (Clause 7.2.2) recommends that organizations deliver regular, role-appropriate security education to reduce human error and encourage a culture of information protection.

Regarding the university, no formal security assessment or user training efforts are described. Despite the SDMS system being accessed by all university employees and the integration of third-party services like EPC, there is no evidence of vulnerability assessments, penetration testing, awareness training, or information security onboarding for staff.

Nonetheless, the presence of role-based access control in the SDMS represents a partial foundation upon which tailored training programs could be developed. Moreover, the centralized infrastructure of the university — with key systems hosted internally — would make it technically feasible to implement centralized assessment and monitoring tools.

6.3. Critique

6.3.1. Pros

- **Existing Role-Based Access Model Indicates a Foundation for Targeted Training:** The university already differentiates access to the SDMS system based on user roles (academic vs. administrative staff). This provides a solid foundation for implementing role-specific security training aligned with each group's privileges and responsibilities.
- **Centralized Systems Offer Easier Scope for Technical Assessment:** With core systems such as the SDMS, the university website, and SU services being hosted internally, security assessments (e.g., vulnerability scans or audits) could be implemented and managed centrally, simplifying the process.
- **Multi-campus Usage of Shared Systems Highlights Need for Assessments:** Although not yet implemented, the fact that both local and remote campuses (e.g., Health and London) access centralized systems shows a clear operational use case for regular security assessments to ensure secure access and consistent policy enforcement.

6.3.2. Cons

- **Lack of Security Awareness Training Across the University:** The University does not mention any cybersecurity training or awareness programs for staff or students, despite their access to sensitive systems such as the SDMS. This increases the risk of human error, phishing, and accidental data exposure.
- **No Evidence of Technical Vulnerability Assessments:** There is no indication that the university performs vulnerability scanning, penetration testing, or system audits. Without these practices, technical flaws may go undetected, leaving critical systems like the SDMS or the university website exposed.
- **No Clear Policy or Control Over Third-Party Services (e.g., EPC):** Although the plagiarism checker (EPC) is hosted externally and contains potentially sensitive academic content, there is no mention of the university conducting security evaluations or compliance checks for this external service.
- **Multiple Access Points Without Mention of Access Review or Assessment:** The SDMS system is accessible by all employees, and other systems are used across departments and campuses. However, the university does not mention any review of access logs or permissions, raising concerns about misuse or over-privileged accounts.
- **No Training for Role-Based Access Enforcement:** While the system enforces role-based access (e.g., academics can't modify data), there is no indication that training is provided to ensure staff understand their permissions and limitations, which could lead to misuse or security bypass attempts.

6.4. Summary

Security assessment and training are critical to ensuring that technical controls are functioning as intended and that users act as responsible custodians of information. Based on the university, this domain reveals notable gaps in current practice. There is no evidence of regular technical assessments, vulnerability scans, penetration testing, or security training for staff and students—despite widespread access to sensitive systems such as the SDMS and third-party tools like EPC.

The lack of training exposes the university to avoidable risks such as phishing, misconfiguration, and privilege misuse. Similarly, the absence of technical reviews may allow undetected vulnerabilities to persist within the infrastructure. These findings reflect a clear misalignment with ISO/IEC 27002:2013 controls (Clauses 7.2.2 and 18.2) and highlight the need for formalized assessment and training programs.

However, the university's centralized systems, internal hosting of key platforms, and the existing role-based access model provide a viable basis for improvement. With the proper implementation of ISO-aligned security assessments and role-specific training, the university can greatly enhance its resilience, compliance posture, and security culture.

7. Security Operations

7.1. Introduction

Security Operations involves a lot of ongoing procedures, tools, and controls to safeguard a university's information and data from any threat or disruption. This includes malware, backup and recovery, software usage control, and incident response. The core systems in the university, such as the SMDS, the SU platform, and the EPC, are accessed by staff, administration, and students in different areas due to the shift online, so the role of security becomes crucial in protecting any data and ensuring integrity, availability, and confidentiality. Several measures and policies must be considered according to BS ISO/IEC 27002:2013 and it will be discussed in this section.

7.2. Review/Overview

Security operations shall be guided and monitored by the policies BS ISO/IEC 27002:2013. They cover areas such as malware protection, data backup, and controlled software usage. Proper implementation of these controls supports system stability, incident readiness, and reduced risk of data compromise.

- **Obtaining Software/Files from External Networks 12.2.1, 12.6.1:** All external software and files must be scanned for malware and reviewed by the IT security before use. It is stated that once a potential risk has been identified, the IT security team should patch any vulnerabilities or add any controls needed to the system.
- **Information Backup Management 12.3.1:** Backup copies essentiality must be created and tested regularly to ensure that they can be recovered in case of any data loss, system failure, or any security breach that can occur. Backups should be stored preferably off-site and away from campus.
- **Restriction on Unauthorized Software Policy 12.6.2:** The university should define and state the approved software that can be installed on any university system. This is due to any uncontrolled installation of software on devices may lead to vulnerabilities in the system, in violation of what was stated before.

Currently, the university lacks a formal policy or consistent implementation for operational activities regarding security operations. It is not mentioned whether any scanning protocols are used when and where backup schedules are scheduled and stored. SDMS enforces a role-based access; it is also not mentioned that they monitor any installed applications and ensure that any secure data recovery procedures are done and ready if any data fails. Despite these gaps, the university's centralized hosting model can ease to deploy unified monitoring, antivirus tools, and backup systems with the SDMS structure the university can control over software access and user actions.

7.3. Critique

7.3.1. Pros

- **Centralized Infrastructure:** The university hosts core systems such as SDMS and SU platforms that are centralized on the university servers. This simplifies the implementation of security controls such as automated backups and malware scanning.
- **Role-Based Access:** Access to the SDMS can ease applying operational controls due to distinguishing between different user groups, where operations such as activity monitoring and software use policies can be enforced and restricted.

7.3.2. Cons

- **No Evidence of Malware Scanning:** Software or documents from external networks are not currently reviewed or scanned, which can pose malware risks to internal systems.
- **No Backup Procedures Defined:** The case study does not mention any backup routines or restoration testing, which can lead to permanent data loss in case of any failure.
- **Unrestricted Software Installation:** There is nothing restricting any software from getting installed. This puts a risk of getting breached, exposed, or deleted in case of any virus.
- **Lack of Oversight for Third-Party Tools:** The case study does not mention any risk assessments done on External Services that are integrated within the system, such as EPC.

7.4. Summary

Effective security operations are critical to ensure the university data and systems remain unattacked by any unauthorized access. However, there is no evidence of any security operations, such as malware scanning and defined backup, happening in the case study. This is all fundamental to secure operations under BS ISO/IEC 27002:2013. These gaps leave the university open to permanently losing data and malware infections. However, with the centralized IT infrastructure and access control models the operations can be conducted regularly and limit any risks coming from any external software.

8. Software Development Security

8.1. Introduction

Software Development security is crucial to maintaining the integrity, confidentiality, and availability of information assets at the university. As the university will rely on custom-developed platforms and third-party tools to support the processes of teaching, learning, and administrating, whether university or student management, the need for secure software development practices is vital. This varies from Student Data Management Systems (SDMS) and Student Union (SU) platforms to academic platforms, and exam platforms. These are highly sensitive data as they include students' records. As per Clause 14.2 of BS ISO/IEC 27002:2013 it clarifies the importance of embedding information security in nearly every phase of the software development life cycle.

This section reviews how software development should be approached within the university, identifies any strengths and gaps, and any flaws that are going to be introduced during the development, deployment, or maintenance, can put the entire data of students and the university at risk.

8.2. Review/Overview

Software development security involves practices done during design, deployments, and throughout any maintenance. The ISO/IEC 27002:2013 standard, especially Clause 14.2, outlines several practices that should be implemented and are relevant to the university's context.

- **Secure Development Policy 14.2.1:** The rules for the development of secure software shall include security in requirements in the design phase, security checkpoints within every milestone, secure code repositories, and in version control systems. Secure programming must be used in any under-development software or production software. '
- **Changes in Systems and Software and 14.2.2, 14.2.4:** In case of any software changes, it must identify all software, information, and database entities that have changed. It must also include risk management, approvals of any change, and an audit description of the whole process. Given that changing software may impact the operations in the universities, it should take place at the right time so that it does not disturb any process related to the university. Compatibility with software already deployed and in use must be ensured. This means that all changes should be fully tested and documented.
- **Secure Development Environment 14.2.6:** The university should create secure environments for system developments across the full life cycle of the development phase. The environments should consider data sensitivity, legal requirements, and any security controls that are already applied. Developers must be trustworthy, and they should monitor any backups, changes, or data movements.

In this use case of the university, development efforts include platforms such as, SDMS, SU platform and academic content systems. The SU should be monitored, and security development measures of the university should be imposed on them, While there is centralization in the infrastructure, there are no secure measures mentioned in the frameworks, code review process, or changes in the software. Also, the reliance on third-party hosted tools like the EPC can raise concerns about secure development standards and the university's ability to control such environments.

8.3. Critique

8.3.1. Pros

- **Centralized Infrastructure:** Hosting systems as SDMS and SU platforms, internally provide an opportunity to enforce such secure development platforms consistently across its systems.
- **Change management Potential:** The university's existing structure, which is divided into administrative, academic, and extracurricular areas, provides a good foundation for establishing a clear way to make software changes more secure.
- **Use of Third-party Tools:** Since the university uses tools like the EPC, it is important to make sure that these tools are connected securely. This encourages the university to be more aware of the risks and should implement proper security checks and measures.

8.3.2. Cons

- **No Formal Development or Modifications Policies:** There is no documentation of how the software should be securely modified or created. This increases the risk of vulnerabilities on all systems that are hosted on the university's servers.
- **Third-party code Risks:** Using external platforms like EPC introduces a danger because these platforms may not have undergone security checks. This is crucial as data sent to external platforms is sensitive information, such as intellectual property and academic significance.
- **No Evidence on Monitoring Development Environments:** There is no indication that the university has secure development environments with controlled access and oversight of the activities done by developers.

8.4. Summary

Software development security is crucial for safeguarding the university's data across the platforms like SDMS, SU, and academic systems. While the centralized infrastructure and structured departments can ease secure practices, there are major concerns such as insecure third-party tools, and unmonitored development environments. The university should follow some of the ISO/IEC 27002:2013 guidelines as stated, but they should also reduce any gaps that can lead to risks regarding data.

9. Guidelines for Cybersecurity Domains

9.1. 1. Introduction

This section outlines practical, domain-specific cybersecurity guidelines for the university described in the case study. These guidelines are based on ISO/IEC 27002:2013 and have been customized to address the university's organizational structure, multi-campus layout, decentralized systems, and blend of on-premise and cloud services. Each domain is represented by one group member and covers clear objectives and actionable steps to improve the university's cybersecurity posture.

9.2. Security and Risk Management Guidelines

9.2.1. Risk Identification and Assessment

Objective: Establish a structured process for identifying and evaluating cybersecurity risks across the university.

Action:

- Conduct annual risk assessments covering all major systems (SDMS, SU server, Lecture Platform).
- Use a standardized risk matrix to evaluate threats based on likelihood and impact.
- Involve representatives from each department and IT unit in identifying critical vulnerabilities.

9.2.2. Security Policy Development

Objective: Create clear, enforceable security policies aligned with university operations.

Action:

- Define acceptable use, data handling, remote access, and password management policies.
- Publish policies on the university intranet and ensure they are accessible to all users.

9.2.3. Incident Response Planning

Objective: Ensure timely and coordinated action during security incidents.

Action:

- Develop an Incident Response Plan (IRP) defining roles, escalation paths, and containment steps.
- Conduct tabletop exercises simulating breaches (e.g., SDMS data breach, phishing attack on SU).
- Maintain a 24/7 incident reporting contact for urgent threats.

9.2.4. Legal and Regulatory Compliance

Objective: Align with national and international data protection laws.

Action:

- Regularly review compliance with GDPR, the Data Protection Act 2018, and academic record laws.
- Appoint a Data Protection Officer (DPO) responsible for ongoing compliance.
- Ensure privacy statements and consent forms are used with student and staff data.

9.2.5. Risk Treatment Planning

Objective: Determine appropriate strategies to mitigate identified risks.

Action:

- For each risk, choose to avoid, reduce, transfer (e.g., via insurance), or accept it with documented rationale.
- Prioritize risks affecting high-impact systems such as SDMS and Wi-Fi infrastructure.
- Track all treatments in a Risk Register reviewed quarterly.

9.2.6. Governance and Oversight

Objective: Maintain high-level control and accountability for security efforts.

Action:

- Form a university-wide Information Security Committee with cross-departmental representation.
- Assign security liaisons in each building (e.g., Shaw, Smallwood, Reeves).
- Report cybersecurity performance and incidents to executive leadership and governing boards.

9.2.7. Risk Communication and Awareness

Objective: Ensure all university users understand key risks and their role in mitigation.

Action:

- Provide risk-based training tailored to user roles (e.g., faculty, admin, IT staff).
- Use newsletters, digital signage, and email campaigns to promote security awareness.
- Share anonymized lessons learned from past incidents.

9.2.8. Continuous Improvement

Objective: Evolve risk and security management over time.

Action:

- Monitor global threats and update university controls accordingly.
- Perform annual audits and update all policies, risk assessments, and plans.
- Solicit feedback from users to improve security processes.

9.3. Asset Security Guidelines

9.3.1. Asset Inventory Management

Objective: Establish and maintain a complete, up-to-date asset register.

Action:

- Record all hardware (e.g., Surface Pros, lab desktops, network devices) and software assets (e.g., SDMS, EPC).
- Include asset ownership, location, classification, and status in the inventory.
- Review and audit the inventory every month.

9.3.2. Asset Classification and Labeling

Objective: Categorize assets based on sensitivity and criticality.

Action:

- Use classification levels: Public, Internal Use, and Confidential.
- Clearly label printed and digital assets, including email disclaimers and file headers.
- Apply handling rules aligned with each classification level.

9.3.3. Data Protection and Encryption

Objective: Safeguard confidential data stored on or transmitted by university assets.

Action:

- Apply full-disk encryption on Surface Pros and all portable devices.
- Use AES-256 or equivalent encryption for stored student data and academic records.
- Enforce SSL/TLS for access to SDMS, email systems, and the cloud-based lecture platform.

9.3.4. Physical Security Controls

Objective: Prevent unauthorized physical access or tampering.

Action:

- Secure servers in locked rooms with CCTV (e.g., Pilling and Reeves Buildings).

- Require cable locks or secured storage for laptops and tablets.
- Implement limited access to sensitive areas like the data center.

9.3.5. Asset Lifecycle Procedures

Objective: Ensure assets are secured from acquisition to disposal.

Action:

- Vet vendors and validate software licenses before procurement.
- Securely configure devices before deployment (e.g., disable unused ports/services).
- Decommission hardware using certified data destruction.

9.3.6. Cloud and Third-Party Asset Control

Objective: Govern assets hosted or accessed via third parties.

Action:

- Require SLAs with EPC and lecture content providers defining encryption, access rights, and retention policies.
- Maintain asset mapping for any university data stored externally.
- Periodically review third-party compliance and access logs.

9.4. Security Architecture & Engineering Guidelines

9.4.1. Architecture Governance and Review

Objective: Embed security into all architectural decisions and life-cycle changes.
Action:

- Establish an Architecture Review Board (ARB) with representatives from IT, information security, and each academic department.
- Require threat modelling and security design reviews for every new system, major upgrade, or cloud migration.
- Maintain an architecture decision register that documents controls, residual risks, and compensating measures.

9.4.2. Segmentation and Isolation

Objective: Prevent lateral movement and contain breaches.
Action:

- Enforce VLANs for each building (Shaw, Smallwood, Reeves, Davenport) and for high-risk systems such as SDMS and SU servers.
- Deploy next-generation firewalls between subnets with deny-by-default ACLs.
- Use jump hosts with MFA for any cross-segment administration.

9.4.3. Cloud Security Controls

Objective: Secure workloads and data hosted outside the main data centre.
Action:

- Require cloud providers (EPC, lecture platform) to implement encryption at rest (AES-256) and in transit (TLS 1.3) and to supply annual SOC 2/ISO 27001 reports.
- Configure cloud security posture management (CSPM) tools to monitor misconfigurations and policy drift.
- Enforce least-privilege IAM roles in the provider's console; disable root or owner keys for daily use.

9.4.4. Endpoint and Device Hardening

Objective: Reduce attack surface on staff PCs, Surface Pros, and lab machines.
Action:

- Apply CIS Benchmarks for Windows, macOS, and Linux images used in teaching labs.
- Enable full-disk encryption and secure boot on all portable devices.
- Use mobile-device management (MDM) to push patches, enforce screen-lock timers, and disable USB mass-storage by default.

9.4.5. Secure Development Lifecycle (SDL)

Objective: Ensure software and configuration code are free of known vulnerabilities.
Action:

- Integrate static (SAST) and dynamic (DAST) security testing into CI/CD pipelines for in-house code supporting the SDMS.
- Require dependency scanning (e.g. Software Composition Analysis) for open-source libraries.
- Maintain a secure code repository with signed commits and protected branches.

9.4.6. Vulnerability and Configuration Management

Objective: Detect and remediate architectural weaknesses promptly.
Action:

- Run authenticated vulnerability scans on SDMS, SU servers, and key network devices each month.
- Track findings in a central ticketing system with risk-rated SLAs (e.g. critical fixes within seven days).
- Perform annual configuration compliance audits against ISO/IEC 27002 control objectives.

9.5. Communication and Network Security Guidelines

9.5.1. Network Segmentation and Access Control

Objective: Isolate systems by department and trust level.
Action:

- Use VLANs and ACLs to segment the SDMS, SU system, and academic buildings.
- Apply firewalls or gateways between sensitive domains.

9.5.2. Wireless Network Security

Objective: Ensure strong encryption and user authentication.
Action:

- Use WPA3 encryption and 802.1X with RADIUS.
- Separate guest and internal Wi-Fi using VLANs.

9.5.3. Secure Data Transmission

Objective: Encrypt all sensitive traffic between systems.
Action:

- Apply HTTPS, SSL/TLS, or VPN tunnels for cloud and cross-campus access.

9.5.4. Logging and Monitoring

Objective: Detect, trace, and respond to threats.
Action:

- Centralize logs from firewalls, SDMS, EPC, and SU systems.
- Monitor and audit logs regularly.

9.5.5. External Service Agreements

Objective: Secure third-party services like EPC.
Action:

- Establish SLAs covering encryption, availability, liability, and audit rights.

9.6. Identity & Access Management Guidelines

9.6.1. Identity Governance Framework

Objective: Provide central oversight of all digital identities across campuses and clouds.
Action:

- Adopt an IAM platform that supports automated provisioning, de-provisioning, and role mapping.
- Define a governance model with clear ownership: HR for staff identities, Registry for students, and IT Security for privileged accounts.

9.6.2. Authentication and MFA

Objective: Strengthen verification of users, especially for remote and privileged access.
Action:

- Mandate MFA (TOTP, push, or FIDO2) for VPN, SDMS admin, and cloud console logins.
- Phase out legacy protocols (POP3, IMAP without OAuth) and weak password policies.
- Enable conditional access rules that trigger MFA based on geo-location or device risk.

9.6.3. Role-Based Access Control (RBAC)

Objective: Align privileges with users' job roles and grades.
Action:

- Map ISO/IEC 27002 "need-to-know" to university grades (Academic, Admin, IT Support, Student).
- Use dynamic groups so that a change in HR or Student Registry automatically adjusts entitlements.
- Review high-risk roles (e.g. SDMS DBA, network engineer) every quarter.

9.6.4. Federated Identity and Single Sign-On (SSO)

Objective: Provide seamless yet secure access to both on-prem and SaaS services.
Action:

- Implement SAML 2.0 / OpenID Connect federation between university IdP and EPC, lecture platform, and any future SaaS.
- Configure just-in-time (JIT) provisioning so that external apps inherit campus roles automatically.
- Require signed and encrypted assertions to protect identity tokens in transit.

9.6.5. Privileged Access Management (PAM)

Objective: Secure and audit elevated credentials.
Action:

- Vault all domain-admin, SDMS-root, and network-device credentials in a PAM solution.
- Force check-in/check-out workflows with session recording for critical changes.
- Rotate privileged passwords automatically after each use or on a 24-hour schedule.

9.6.6. Identity Lifecycle and Off-boarding

Objective: Ensure timely removal of access for leavers and role changers.
Action:

- Integrate IAM with HR and Student Registry feeds for real-time status updates.
- Disable accounts within eight hours of contract termination or graduation.
- Run monthly orphan-account reports and remediate within 48 hours.

9.6.7. Monitoring and Audit

Objective: Detect misuse of credentials and enforce accountability.
Action:

- Send all IAM and authentication events to a central SIEM for correlation.
- Enable anomaly-detection rules (e.g. impossible-travel, brute-force MFA failures).
- Retain audit logs for at least 12 months to satisfy academic and legal record-keeping requirements.

9.7. Security Assessment & Training Guidelines

9.7.1. Role-Based Security Training Program

Objective: Ensure that staff and students are trained based on their specific access level and responsibilities.
Actions:

- Develop separate training modules for academic staff, administrative staff, IT personnel, and students.
- Cover topics like phishing, password hygiene, data handling, and system usage policies.
- Require completion during onboarding and renew training annually.

9.7.2. Security Awareness Campaigns

Objective: Reinforce secure behavior through ongoing education.
Actions:

- Run quarterly awareness campaigns using posters, emails, and videos.
- Include simulated phishing attacks to test awareness.
- Publicly recognize departments with high participation rates.

9.7.3. Regular Technical Security Assessments

Objective: Identify vulnerabilities and misconfigurations proactively.
Actions:

- Perform vulnerability scans on internal systems like SDMS, SU servers, and the university website.
- Schedule annual penetration testing by third-party professionals.
- Document findings and enforce a remediation timeline.

9.7.4. Periodic Review and Audit of Access Privileges

Objective: Ensure staff have only the access they need.
Actions:

- Review user permissions to the SDMS, EPC, and internal systems every 6 months.
- Remove or adjust access for staff who change roles or leave.
- Maintain logs of all access changes and reviews.

9.7.5. Security Requirements for Third-Party Services

Objective: Ensure cloud providers like EPC meet security standards.
Actions:

- Sign SLAs with clear clauses on encryption, incident reporting, audit rights, and data handling.
- Conduct annual reviews or request security compliance reports from providers.
- Prohibit integration of third-party tools without a formal security evaluation.

9.7.6. Monitor and Measure Training Effectiveness

Objective: Track participation and adjust training based on results.
Actions:

- Log training completion rates per department.
- Use pre- and post-training quizzes to assess knowledge retention.
- Analyze phishing simulation outcomes and update awareness content accordingly.

9.7.7. Assign Responsibility for Assessment and Training

Objective: Ensure accountability for program management.
Actions:

- Appoint a Security Awareness Officer or designate a training lead within the IT department.
- Require each department to nominate a cybersecurity liaison.
- Define roles and reporting structures clearly within the university's ISMS.

9.8. Secure Operations Guidelines

9.8.1. Malware Protection

Objective: Ensure that all software and files from external sources are screened for malware and security threats before being downloaded and executed on the university system and data.
Actions:

- Scan all external files and software with anti-malware solutions

- Require IT security team approval before installing any non-standard applications.
- Enforce automatic updates for anti-malware software on all university devices.

9.8.2. Information Backup Management

Objective: Ensure regular and recoverable backups to be able to proceed in any case that data loss happens due to failure or attacks.
Actions:

- Perform automated and scheduled backups, especially for all the core systems like academic platforms, SDMS, and SU systems.
- Store backup copies off-site or in a secure cloud location. This should be stored away from the main university network.
- Regularly test backup restoration for data to ensure availability and a smooth process in case of any data loss.

9.8.3. Restriction on Unauthorized Software

Objective: Minimize any security risk associated with the installation of unauthorized software.
Actions:

- Define a list of approved and authorized software for academic and administrative use.
- Monitor systems regularly for any unapproved software, and if unauthorized programs are found, they must be removed.

9.9. Software Development Security Guidelines

9.9.1. Secure Software Development Life-cycle

Objective: Ensure the security is integrated into every phase of the software development life cycle. From the design phase to developing and deploying, and finally, maintenance.
Actions:

- Define security requirements in the design phase
- Include security in milestones or sprints
- Use version control systems that require secure login credentials and track any changes.
- Enforce secure coding standards.

9.9.2. Change and configuration Management

Objective: Control and document all changes to software systems to reduce risks of operational disruptions
Actions:

- Assess and document risks before implementing.
- Testing changes in isolated environments before deploying.
- Document all changes and modifications..

9.9.3. Secure Development Environments

Objective: Maintain isolated, access-controlled development environments that protect sensitive data against any unauthorized access or leakage
Actions:

- Restrict access to development environments to authorized personnel only.
- Live production data should not be used in development environments.
- Monitor development environments for any data movements or changes that should not be done.

9.9.4. Third-party programs use

Objective: Evaluate any third-party tools and platforms before integration into the university systems.
Actions:

- Ensure that third-party tools are in line with university security policies.
- Check that the outside software is not known for any security problems.

Individual Contribution

The table below summarizes each group member's assigned domain in this cybersecurity case study report.

Group Member	Cybersecurity Domains and Guidelines
Toqa Mahmoud	Security & Risk Management
Toqa Mahmoud	Asset Security
Merna Hebishy	Security Architecture & Engineering
Merna Hebishy	Identity & Access Management (IAM)
Adham Salem	Communications & Network Security
Adham Salem	Security Assessment & Testing
Ismail Sabry	Security Operations
Ismail Sabry	Software Development Security

Table 2: Individual Contributions Based on Cybersecurity Domains and their corresponding Guidelines

References

1. *British Standards Institution* (2013) *BS ISO/IEC 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements.*
2. *British Standards Institution* (2013) *BS ISO/IEC 27002:2013 - Code of practice for information security controls.*
3. *British Standards Institution* (2010) *BS ISO/IEC 27003:2010 - Information technology – Security techniques – Information security management system implementation guidance.*
4. *British Standards Institution* (2009) *BS ISO/IEC 27004:2009 - Information technology – Security techniques – Information security management – Measurement.*
5. *National Institute of Standards and Technology* (2014) *NIST Special Publication 800–88 Revision 1: Guidelines for Media Sanitization.* Gaithersburg, MD: U.S. Department of Commerce.
6. Chen, X., Brown, G. and Hu, S. (2021) ‘Implementing defence-in-depth for higher-education networks’, *Computers Security*, 105, 102249.
7. Davis, P. (2024) ‘Endpoint security challenges in blended-learning environments’, *Journal of Information Security and Applications*, 73, 103473.
8. EDUCAUSE (2020) *Higher-ed cybersecurity guide: Preparing for online and blended learning.* Washington, DC: EDUCAUSE.
9. European Union Agency for Cybersecurity (ENISA) (2021) *Guidelines for securing the ICT supply chain.* Athens: ENISA.
10. International Organization for Standardization and International Electrotechnical Commission (2013) *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.* Geneva: ISO.
11. National Institute of Standards and Technology (2022) *NIST SP 800-160 Rev. 1: Systems Security Engineering.* Gaithersburg, MD: NIST.
12. Patel, R. and Green, L. (2022) ‘Secure software development lifecycle adoption in academic institutions: a case study’, *Information and Software Technology*, 145, 106825.
13. Smith, M. and Jones, A. (2023) ‘Zero-trust architectures in university networks’, *Journal of Cyber Security Technology*, 7(2), pp. 85–104.
14. UK Information Commissioner’s Office (ICO) (2024) *Guide to the UK GDPR.* Wilmslow: ICO.
15. Williams, D. (2020) ‘Cloud data residency and GDPR compliance in UK higher education’, *International Journal of Information Management*, 54, 102186.

16. Chen, X., Brown, G. and Hu, S. (2021) ‘Implementing defence-in-depth for higher-education networks’, *Computers Security*, 105, 102249.
17. Davis, P. (2024) ‘Endpoint security challenges in blended-learning environments’, *Journal of Information Security and Applications*, 73, 103473.

18. EDUCAUSE (2020) *Higher-ed cybersecurity guide: Preparing for online and blended learning.* Washington, DC: EDUCAUSE.

19. European Union Agency for Cybersecurity (ENISA) (2021) *Guidelines for securing the ICT supply chain.* Athens: ENISA.

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

21. Joint Information Systems Committee (JISC) (2021) *Federated identity management for UK higher education.* Bristol: JISC.

22. National Cyber Security Centre (NCSC) (2023) *Multi-factor authentication guidance.* London: NCSC.

23. National Institute of Standards and Technology (2022) *NIST SP 800-160 Rev. 1: Systems Security Engineering.* Gaithersburg, MD: NIST.

24. Patel, R. and Green, L. (2022) 'Secure software development lifecycle adoption in academic institutions: a case study', *Information and Software Technology*, 145, 106825.

25. Smith, M. and Jones, A. (2023) 'Zero-trust architectures in university networks', *Journal of Cyber Security Technology*, 7(2), pp. 85–104.

26. Syreyshchikova, A., Higgins, O. and O'Reilly, M. (2020) 'Identity and access management in higher education: challenges and best practices', *International Journal of Information Management*, 54, 102216.

27. UK Information Commissioner's Office (ICO) (2024) *Guide to the UK GDPR.* Wilmslow: ICO.