

AUDIT REPORT

Security Audit of Computing Resources –

Recipients:

TO: Robert Beadle, Chief Auditor

FROM: Nayomi Furtado, Auditor

Date: 27th March 2025

This report represents a true statement of the audit findings and conclusion.

Table of Contents

Section 1: Scope.....	1
Section 2 : Business Setting	2
Section 3 : Practical Audit Method Employed	3
Section 4 :Secure Areas	6
4(a) Expected Controls	6
4(b) Observed Controls and Comments	7
Section 5 : Equipment Security.....	9
5(a) Expected Controls	9
5(b) Observed Controls and Comments	10
Section 6 : Audit Conclusion	12
6(a) Overall conclusion based on relevant GAP analysis	12
6(b) Recommendation for Immediate and Future Management Action	13
References.....	16
Appendix A: Work-In-Progress Notes.....	17
Appendix B: Security Checklist.....	19
Appendix C: Photographic Evidence	21

Section 1: Scope

This audit evaluates the physical security and equipment security of all the computing resources within the [REDACTED]. The main goal is to assess the effectiveness of physical controls in protecting computing resources against unauthorized access, damage, and interference, as well as to examine equipment security measures to prevent theft, misuse, or operational disruption.

The audit will involve direct observation and comparing findings with the ISO27002:2022 Section 7 standards, which focus on secure areas and equipment security. Observations will be made discreetly to avoid alerting technical staff, ensuring an objective and thorough assessment of the existing security posture. A checklist-based approach will guide the assessment to ensure that all relevant controls are thoroughly examined.

This audit will focus on physical security measures for student-accessible computing laboratories, including security perimeters, physical entry controls, proper device placement, and the protection of essential utilities like power and cabling. It will also evaluate environmental safeguards, such as fire safety measures, ventilation, and workspace organization. This audit will only cover areas accessible to students, excluding staff offices, seminar rooms, and other restricted spaces. It will not cover operating systems, network security, or server infrastructure, as it is solely focused on physical security.

The audit will find weaknesses in physical security and equipment and provide recommendations to improve security and protect the resources in the [REDACTED].

Section 2 : Business Setting

This audit focuses on the Department of Computing and Mathematical Sciences (CMS) at the [REDACTED]. It examines the physical security of the computing laboratories located in the [REDACTED] Building, where CMS students regularly carry out practical work and research. These labs are managed by the department and play an important role in supporting hands-on learning as part of the university's academic activities.

The CMS department offers a variety of technology-related courses. These include Computer Science, Cybersecurity, Software Engineering, Artificial Intelligence, and Data Science. Many of these courses involve hands-on work, so students need regular access to reliable computing resources.

The computing labs are available mainly to CMS students and staff. Access to the labs is controlled using university ID cards, which must be scanned to enter the building and the rooms. This helps prevent unauthorised people from entering. The labs are generally open from 8:00 in the morning to 9:00 at night on weekdays. During weekends and university holidays, lab access is fully restricted to ensure security and proper maintenance.

This audit is carried out to understand how secure these physical spaces are. It checks whether access controls are working properly, whether the equipment is safe, and whether the environment is well-managed. The goal is to find and fix any weaknesses in the current system so students and staff can continue to use the labs in a safe and secure way throughout their academic activities.

Section 3 : Practical Audit Method Employed

The audit of the physical security controls for the [REDACTED], Building computing resources was conducted using a clear and evidence-based method. The focus was on key areas such as access control, physical barriers, surveillance, and equipment security, in line with the guidelines of ISO27002:2022, Section 7. The audit involved visual inspections, note-taking, and sampling to assess how well the current security measures are working. A representative range of areas within the building was reviewed, and the security was evaluated at different times of the day to see if it remained consistent and effective. The methodology is outlined below:

1. Preparation and Planning:

- A review of ISO27002:2022, Section 7 was undertaken to understand the expected physical security controls, including those related to secure areas and equipment security. Key areas of focus included access control, physical barriers, monitoring systems, and asset protection.
- Existing security policies and guidelines provided by the University of [REDACTED] were also reviewed to align the audit criteria with the institution's current practices. This ensured that the audit reflected both the best practices outlined in ISO27002:2022 and the institution's internal security protocols.
- A comprehensive audit checklist was developed based on the ISO27002:2022 framework to systematically evaluate the observed physical security measures and identify any deviations from the expected standards.

2. Observational Data Collection:

Observations were performed directly in the computing laboratories during standard operating hours. A combination of real-time note-taking and photographic documentation was used to capture key aspects of physical security, such as access control measures, physical barriers, surveillance systems, cabling etc.

Particular attention was given to points of entry, critical equipment storage areas, and visual observation of surveillance coverage. The key areas assessed included:

- **Access Control:** Observation of physical security measures at entry points to secure areas, including locks, card readers, and biometric access.
- **Physical Barriers:** Inspection of doors, walls, and partitions that protect secure areas from unauthorized access.
- **Surveillance Systems:** Evaluation of the presence and visibility of security cameras and alarms systems.
- **Equipment Security:** Assessment of physical security for devices such as computers, cables, printers, and peripheral devices, with particular attention to physical locks and other protective measures.

3. Gap Analysis:

- The observed physical controls were compared against the requirements outlined in ISO27002:2022, as well as the ██████████ internal security policies, to identify gaps in security. The analysis aimed to detect discrepancies such as unsecured areas or equipment, flaws in access control measures.
- This prioritization ensured that the most important vulnerabilities, such as those affecting critical equipment or busy areas, were addressed first.

4. Audit Techniques:

- A detailed checklist was used to document the observations made during the audit, ensuring that all relevant security measures were evaluated. This approach provided consistency and accuracy in documenting findings (see Appendix B).
- Photographic evidence was used to visually document key observations, providing clear evidence to support the assessment (see Appendix C).
- The audit employed a structured, methodical approach to ensure all key areas of the premises were thoroughly assessed, focusing on secure areas, access points, and critical equipment storage.
- Work in progress reports were used to track the audit's progress, ensuring that all areas were covered and allowing for timely adjustments as necessary (see Appendix A).

5. Sampling Methodology:

- A representative sampling approach was used to cover all three floors of the ██████████ with a focus on the first and second floors where the computing labs are located. This ensured that all key areas were assessed for physical security. The sampling helped evaluate both busy areas and less frequently used spaces, ensuring a thorough review of the building's security.

6. Observations Across Different Times:

- The audit was conducted at different times during the day to assess whether security measures varied during peak and off-peak hours. Observations were made during early mornings, mid-day, and late afternoons, capturing different activity levels within the computing laboratories.
- The purpose of observing at different times was to evaluate how security measures perform during busy periods like class hours and quieter times like after hours, providing a better understanding of their effectiveness and reliability.

7. Documentation and Reporting:

- All findings were carefully documented and organized, with detailed records kept of every observation made.
- The audit report presents the findings in a structured manner, with clear comparisons between the expected and observed physical controls, highlighting gaps, risks, and recommendations for improvement.

Section 4 :Secure Areas

In accordance with ISO 27002:2022 and the University of ██████████ internal policies, secure areas are designed to prevent unauthorized access, theft, damage, or compromise of assets, especially sensitive information stored within computing facilities. This section examines the physical security measures in place for the computing laboratories in the ██████████ Building. It focuses on who has access to these areas, how the rooms are secured, and any potential environmental risks that could affect the safety and functionality of the equipment.

4(a) Expected Controls

The expected controls for secure areas in the computing laboratories aim to ensure the protection of sensitive information and assets. These controls include physical security measures, access restrictions, environmental protections, and clear operational guidelines to safeguard the labs and their contents.

1. **Physical Barriers and Perimeter Security**

The computing resources should be surrounded by secure walls, doors, and windows creating a protective barrier around the sensitive equipment and information. Also, external doors and windows should be fitted with reinforced locking mechanisms to prevent unauthorized access. The areas around the entrances and walkways should be well-lit, with working lights to make sure the area is visible and secure, especially at night.

2. **Entry Control Systems**

The entry points of the building and computing laboratories should have access controls like locks, card readers, or biometric scanners to make sure only authorized people can get in. ID display requirements at entry points should be enforced for secure areas. Additionally, tailgating prevention measures such as anti-tailgating doors or barriers should be present to prevent unauthorized persons from entering after an authorized person.

3. **Securing the Labs and Facilities**

Sensitive physical and electronic data must be stored securely in safe areas or room which should always remain locked and should ensure only authorized individuals have access to them. Clear security signage must be displayed to warn against unauthorized access. Clear signs indicating restricted access like "No Unauthorized Access" or "Restricted Area" should be posted to prevent accidental or intentional unauthorized entry. Also, Emergency exits should be clearly marked and easily accessible in case of an evacuation. These exits should be free from obstructions but must also be secured to prevent unauthorized access. Surveillance cameras should be placed in and around the lab areas to monitor unauthorized access.

4. **Security Awareness and Work Practices**

Ensure that there are clear guidelines posted or provided to staff and students on how to handle sensitive data or equipment in the lab or near computing or electronic devices. Also, observing whether the students and staff are following these guidelines, such as locking computers when not in use, not leaving sensitive information on display, and using secured storage for sensitive materials.

4(b) Observed Controls and Comments

This section outlines the physical security measures observed during the audit. It focuses on the existing controls, how effective they are, and areas that may need improvement. The observations cover security barriers, access control and staff adherence to security procedures. The following controls were observed:

1. **Physical Barriers and Perimeter Security**

The ██████████ Building, which contains computing resources across multiple floors, has solid walls, secure doors, and windows that act as physical barriers against unauthorized access and environmental risks. The doors leading to computing laboratories, offices, and other facilities are fitted with locks, and some have self-closing mechanisms to prevent them from being left open, as shown in Figure 2 (refer to the Appendix). However, some doors, including those inside the computing laboratories, lack reinforced locking mechanisms or are made of glass, making them more vulnerable to forced entry or unauthorized access, as shown in Figure 3 (refer to the Appendix). The walkways and entrances around the building are well-lit, reducing the risk of unauthorized activities during low-visibility hours. All outdoor and hallway lighting was operational, with no reported failures at the time of inspection.

2. **Entry Control Systems**

The main entrance to the ██████████ Building is access-controlled, requiring an access ID card for entry, as shown in Figure 1 (refer to the Appendix). This prevents unauthorized individuals from freely accessing the facility. However, once inside, no further authentication is required to enter the computing laboratories or access computing resources. In some cases, individuals can enter the labs without displaying an ID card, as there are no additional access controls, such as biometric authentication or PIN-based systems, for extra verification. This lack of extra checks means a lost or stolen ID card could be used by someone else. Another issue is tailgating, where an unauthorized person can follow someone with an ID card into restricted areas. Since there are no turnstiles, man-trap doors, or other barriers, it's easy for someone to enter the computing laboratories without proper checks. Improving internal access controls would help make the building more secure.

3. **Securing the Labs and Facilities**

During the audit, it was observed that certain restricted areas, such as the data rooms and the electrical riser cupboard, were properly secured and consistently remained locked, as seen in Figure 4 and 5 (refer to the Appendix). This ensures that only authorized personnel can access these areas, providing an essential control to protect sensitive data and equipment. However, it was noted that some restricted areas, particularly the data rooms, lack visible signage indicating restricted access, as seen in Figure 4 (refer to the Appendix). The absence of clear signage means there is no immediate indication that entry is limited to authorized personnel only. This could lead to confusion or accidental entry by unauthorized individuals, posing a potential security risk. While the emergency exits were well-marked and free from obstructions, ensuring

safe evacuation in case of an emergency, the computing laboratories lacked clear signage, such as "No Unauthorized Access" or "Authorized Personnel Only," near entrances or around sensitive equipment. These signs are crucial to reinforce security policies and communicate restricted access, and their absence increases the risk of unauthorized entry. CCTV cameras were installed in key locations, including near entrances and within the computing labs, providing passive surveillance. However, it remains unclear whether security personnel actively monitor the footage in real-time or if it is only reviewed after an incident occurs.

4. Security Awareness and Work Practices


During the audit, several security awareness posters were observed throughout the entire [REDACTED] Building, including the computing laboratories. These posters helped to promote security, as seen in Figure 6, 7 (refer to the Appendix). In addition, a fire action plan was visibly posted in key areas, ensuring that emergency procedures were easily accessible to staff and students, as seen in Figure 8 (refer to the Appendix). Both students and staff were generally adhering to the security guidelines posted in the labs, with screens consistently locked when students left their workstations, demonstrating good security practices. No sensitive data was left exposed, and students appeared cautious with their personal information. These observations suggest that both students and staff are aware of the security guidelines, and the presence of the posters, is having a positive impact in promoting good security practices throughout the building.

Overall Security Impact and Compliance

The current physical security measures in place provide a reasonable level of protection for the computing laboratories. The access control system, which requires an ID card for entry, ensures that only authorized individuals can enter. The well-lit surroundings contribute to a secure environment, and staff and students generally adhere to security guidelines, demonstrating an understanding of the importance of maintaining lab safety. The presence of CCTV cameras enhances security, though it is unclear whether footage is actively monitored, which limits its effectiveness in preventing incidents in real-time. Additionally, the use of glass doors in some areas and the lack of reinforced locking mechanisms on certain doors, including those within the labs, pose potential security vulnerabilities.

From a compliance perspective, the security measures meet several aspects of ISO 27002:2022 guidelines, particularly regarding physical security and access control. However, the absence of biometric authentication, real-time video monitoring, and clear signage in restricted areas prevents full compliance. While these gaps exist, the overall security system still ensures a secure and well-organized environment for both students and staff. To strengthen the security posture, it is recommended to implement additional measures, such as integrating biometric authentication for more secure access, establishing real-time monitoring of CCTV footage, and adding clearer signage to restricted areas. These improvements would address the current vulnerabilities and better align the system with ISO 27002:2022 compliance.

Section 5 : Equipment Security

To ensure the protection and reliability of computing equipment in the  Building laboratories, several security controls should be in place. These controls focus on minimizing environmental risks and ensuring continuous operation.

5(a) Expected Controls

The following expected controls align with ISO 27002:2022 requirements and ensure equipment remains secure and functional.

1. **Secure Placement and Protection of Equipment**

All IT equipment should be placed in secure locations to prevent theft, damage, or unauthorized access. Workstations, wires and network devices must be kept in controlled areas with restricted access. Equipment should not be left in public spaces or unsecured areas where it could be tampered with or stolen. Fire suppression systems should be installed to reduce potential hazards. Unused IT equipment should be securely stored in locked cabinets or designated storage areas to prevent unauthorized access.

2. **Protection Against Power and Environmental Controls**

To ensure IT equipment is protected from power disruptions that may lead to data loss or system failures, backup power solutions, such as Uninterruptible Power Supplies (UPS) or generators, must be in place. These solutions guarantee continuous operation during power outages. The electrical infrastructure should be designed to safely support power loads, avoiding the use of overloaded sockets or excessive reliance on extension cords, which could present hazards. Surge protectors must be installed across critical equipment to shield against power surges. Furthermore, sufficient power outlets should be provided to support all computing devices, minimizing the need for multiple extension cords or multi-plug adapters, which could lead to overloading.

In addition to power protection, environmental controls are essential for maintaining equipment integrity. Effective temperature and airflow management must be implemented to prevent overheating. This includes using air conditioning or ventilation systems to regulate temperature and ensure optimal environmental conditions for IT equipment.

3. **Cabling Protection and Security**

Power and network cables should be installed securely to prevent damage, disconnection, or unauthorized tampering. Cables should not be left loosely placed across desks or floors, where they could be easily pulled or cause tripping hazards. Instead, they should be routed through protective conduits, cable trays, or structured cabling systems. To enhance security, network and power cables must be shielded from unauthorized access to reduce the risk of potential breaches. Whenever possible, cabling pathways should be enclosed to prevent tampering or interception. All cables should be organized, clearly labelled, and securely fastened to avoid entanglement or damage. A well-structured cabling system improves reliability and minimizes the chances of service disruptions.

5(b) Observed Controls and Comments

This section evaluates the physical security measures for protecting IT equipment. It examines existing controls, their effectiveness, and areas for improvement, focusing on equipment placement, protection methods, and adherence to security protocols. The following controls were observed:

1. Proper Placement and Protection of Equipment

The computing resources were found in open-access labs, with no clear separation or distinction from adjacent areas, potentially exposing them to unauthorized access or theft. In some labs on the upper floor, systems such as CPUs and desktops were securely embedded into the desks and locked, effectively preventing theft as seen in Figure 9 (refer to the Appendix). However, in other labs on the lower floor, the systems, including CPUs and monitors, were unsecured to the desks, which posed a risk of theft as seen in Figure 10 (refer to the Appendix). Also, the systems were placed too close to each other, which increased the risk of shoulder surfing. This setup allowed unauthorized individuals to easily view sensitive information on nearby screens, as seen in Figure 11 (refer to the Appendix). Additionally, a portable air conditioner was observed in the open area of the lab with an "Out of Order" sign attached, indicating it was not functional as seen in Figure 12 (refer to the Appendix). Non-operational equipment, such as this, should not remain in active work areas. These items should be promptly removed and stored in designated, separate areas to prevent confusion, minimize potential hazards, and avoid obstruction of walkways or disruption to the workspace environment. Fire safety measures were robustly in place, with fire extinguishers and alarms strategically located and in good working condition. These safety devices were easily accessible, and a fire action plan was prominently displayed in visible areas, clearly outlining evacuation procedures and safety protocols to follow in the event of an emergency.

2. Protection Against Power and Environmental Controls

During the audit, there was no visible indication of Uninterruptible Power Supply (UPS) systems or surge protection equipment in the computing areas. However, the electrical infrastructure appears to be well-designed to handle power loads, with properly installed power distribution panels and circuits. There were sufficient power outlets and extension cables available to distribute the power load across devices as seen in Figure 14 (refer to Appendix). Surge protectors were observed in use across critical equipment, which helps mitigate the risk of damage from potential power surges. The computing areas were adequately ventilated, with ceiling vents in place to ensure proper airflow and temperature regulation. Additionally, posters on the windows emphasized the importance of keeping windows open for improved ventilation, as seen in Figure 15 (refer to Appendix). The windows were fitted with blinds, effectively controlling sunlight and reducing glare, while still allowing sufficient airflow to maintain a comfortable and optimal working environment.

3. Cabling Protection and Security

During the audit, it was observed that most cables were loosely placed across desks, presenting potential risks such as damage, disconnections, and tripping hazards. In some areas, wires were loosely attached to CPUs and monitors, which increases the risk of physical damage. Additionally, some cables were entangled, creating possible obstructions and wear, as seen in Figure 16 (refer to Appendix) . However, in several areas, network and power cables were properly routed through protective conduits, cable trays, or structured cabling systems, which helps reduce the risk of damage or tampering, as seen in Figure 14 (refer to Appendix). Unused IT cables were found loosely stored in an open cupboard, which could pose safety hazards and allow for unauthorized access, as seen in Figure 13 (refer Appendix). Furthermore, the electrical riser cupboard, which contains critical cabling and electrical infrastructure, was securely locked, ensuring that unauthorized individuals could not access sensitive connections. While some areas followed best practices for cabling, it is recommended to address the issues of loose cables, entanglement, and improper storage to improve overall security and safety.

Overall Security Impact and Compliance

The physical protection of IT equipment in the laboratories is generally adequate, though certain areas present security risks. While systems in some labs are securely embedded into desks and properly organized, other areas exhibit unsecured equipment, increasing the potential for theft or tampering. Loose cables and improperly stored unused equipment also pose safety hazards and may cause operational disruptions.

From a compliance point of view, the observed controls partially align with the ISO 27002:2022 guidelines, particularly regarding basic equipment placement and fire safety measures. However, issues such as unsecured devices, improper cable management indicate non-compliance with key security protocols. To improve the overall security posture and ensure full compliance with ISO 27002:2022, it is recommended to address the vulnerabilities related to equipment security, enhance cable management practices, and introduce surge protection and backup power systems where needed.

Section 6 : Audit Conclusion

6(a) Overall conclusion based on relevant GAP analysis

Below is the gap analysis based on the observed security measures. The table outlines the compliance level for each security control, highlighting areas that require attention and indicating the overall gap in security compliance.

Security Measure	Good (75-100%)	Needs Some Attention (25-75%)	Needs Much Attention (0-25%)
Are physical barriers (walls, secure doors, windows, and lighting) in place to prevent unauthorized access?		70	
Is there an effective entry control system, including access cards, biometric authentication, and tailgating prevention?		30	
Are clear and visible signs posted for restricted areas, unauthorized access warnings, and emergency exits?		60	
Are CCTV cameras present, and is it covering all the required areas of the building and entry points?		70	
Are staff and students following security awareness guidelines (e.g., screen locking, no exposed data, awareness posters)?	75		
Are fire safety measures in place, including fire extinguishers, alarms, and a visible fire action plan?	75		
Is IT equipment properly secured, including structured cabling, locked storage, and removal of non-operational equipment?		50	
Are power and environmental controls (e.g., ventilation, surge protection, power management) properly implemented?		50	
	150	330	
480 % of possible 800% = 480/800 = 60% compliant so, GAP is 100-60= 40%			

The gap between the expected and actual findings was 40%, with an overall compliance rate of 60%. While certain areas, such as fire safety, security awareness, and physical barriers, met expectations, significant deficiencies were identified in entry control systems, IT equipment security, and access restrictions.

The most notable gap was in entry control, where the absence of multi-factor authentication (MFA) and weak internal access controls created vulnerabilities. IT equipment security also fell short, with unsecured computing resources in some areas, increasing the risk of theft or tampering. Additionally, cabling security and environmental controls needed improvement to prevent damage, unauthorized access, and operational disruptions.

Bridging this 40% gap will require enhanced access control, stricter IT equipment security, improved cabling management, and the implementation of stronger authentication mechanisms

to align with best practices and industry standards, ensuring a more secure and resilient environment.

6(b) Recommendation for Immediate and Future Management Action

1. **Entry Control System and Unauthorized Access Prevention**

Currently, the building employs a basic entry control system that relies on the display of an ID card for access. This system allows individuals with authorized ID cards to enter the building and move freely between various areas, including computer labs. While this method ensures basic access control at the main entrance, it presents a security gap. Once inside, there are no further barriers to prevent unauthorized individuals from entering sensitive areas like computer labs. This leaves computing resources vulnerable to potential security breaches, as anyone with an ID card can enter restricted zones without further verification. The absence of additional control increases the risk of unauthorized access to confidential data, theft of equipment, or even property damage within these areas.

Recommendations:

To improve security and prevent unauthorized access to critical areas, it is recommended to implement a tap-in mechanism at the entrances to sensitive zones like computer labs. This system would require individuals to tap their ID card against a reader for additional verification before gaining access. This added layer of authentication reduces the risk of unauthorized entry, as it ensures that only authorized individuals with valid ID cards are granted access. Implementing turnstiles or mantraps at key access points would further ensure that only one person enters at a time, preventing tailgating and further securing restricted areas. The benefits of this system include enhanced security, improved monitoring of access to sensitive areas, and the reduction of security breaches and unauthorized access. Additionally, this solution is cost-effective, leveraging existing ID infrastructure and providing a simple yet powerful enhancement to building security.

Cost/Benefit:

A tap-in system is a cost-effective upgrade compared to biometric solutions. It utilizes the existing ID card infrastructure while adding a layer of security. The installation of turnstiles or mantraps at high-risk access points is also a relatively low-cost solution that significantly enhances security by preventing unauthorized entry. Over time, the reduced risk of security breaches and the protection of valuable resources make this solution both financially beneficial and a worthwhile investment.

Follow-Up Actions:

- Install tap-in card readers and turnstiles at all sensitive entrances.
- Remove the old ID display-only system in sensitive areas and inform all staff about the new access process.
- Do a risk assessment 3 months after installation to check if unauthorized access has decreased.

- Have security teams review entry logs weekly and update access policies. Train staff on the new procedures.

2. IT Equipment Security and Structured Cabling

The audit revealed several concerns related to IT equipment security and cabling management, both of which could expose the organization to physical and security risks. In the labs, IT equipment such as CPUs and desktops were found in open-access areas without adequate physical security, making them vulnerable to theft or unauthorized tampering. Systems were also placed too closely together, increasing the risk of shoulder surfing, where unauthorized individuals can easily view sensitive information on screens.

Additionally, cabling practices in certain areas were inadequate. Cables were loosely placed across desks, some were entangled, and unused cables were stored openly in cupboards. These practices increase the risk of physical damage, disconnections, tripping hazards, and unauthorized access to potentially sensitive infrastructure. While some areas adhered to best practices with structured cabling systems, others still posed significant safety and security concerns.

Recommendations:

- Secure IT Equipment: Mounting all IT systems (CPUs, monitors) securely to desks using locks, brackets, or other mounting. Where possible, embed systems into desks or use cable locks for portable equipment. This will prevent the theft or unauthorized removal of IT equipment, tampering with systems, and reduce the risk of data theft or unauthorized access to sensitive information.
- Reduce Shoulder Surfing Risk: Reconfiguring system placement to create adequate space between workstations or using privacy screens on monitors will help protect sensitive data from unauthorized viewing, minimizing the risk of data breaches and information leaks due to shoulder surfing.
- Address Cable Safety: Secure loose cables and prevent entanglement by routing them through cable trays or protective conduits. Store unused cables in locked cabinets or designated spaces to eliminate tripping hazards, accidental disconnections, physical damage, and unauthorized access, reducing the risk of theft or tampering.

Cost/Benefit:

Securing IT equipment by mounting systems and improving cable management, represent a relatively low-cost investment compared to the potential risks of theft, unauthorized access, equipment damage, or operational disruptions. The long-term benefits of implementing structured cabling will significantly reduce the likelihood of security breaches, equipment malfunctions, and safety hazards. Moreover, these improvements will create a safer working environment, lower repair costs, and reduce the risk of workplace accidents, thus delivering substantial value over time.

Follow-Up Actions:

- Install mounting brackets and privacy screens.
- Remove all loose cables and secure any exposed equipment to prevent theft or damage. Put in place clear policies for keeping IT equipment safe and organized.
- Provide training for IT and facilities staff on how to maintain equipment security and proper cable management. Make sure procedures are updated and easy to follow.

3. Physical Barriers

Physical barriers, such as walls, secure doors, windows, and lighting, are the first line of defence against unauthorized access to the building. The organization has implemented solid physical security measures, including locked doors and windows, which provide basic protection against intrusions. The presence of well-lit walkways and entrances enhances visibility, reducing security risks during low-light conditions. However, certain vulnerabilities were identified. Some doors lack reinforced locking mechanisms, making them susceptible to forced entry. Additionally, the laboratory IT support office doors are made of glass, which increases visibility into restricted areas and makes them more vulnerable to break-ins or unauthorized access.

Recommendations:

Doors with glass panels should be fitted with shatter-resistant film or replaced with more secure materials, making it significantly more difficult to break, thereby delaying or deterring forced entry attempts. Replacing glass doors with solid-core or reinforced materials eliminates visibility into secure areas, preventing unauthorized individuals from observing sensitive activities or targeting valuable IT assets, thereby enhancing overall security.

Cost/Benefit:

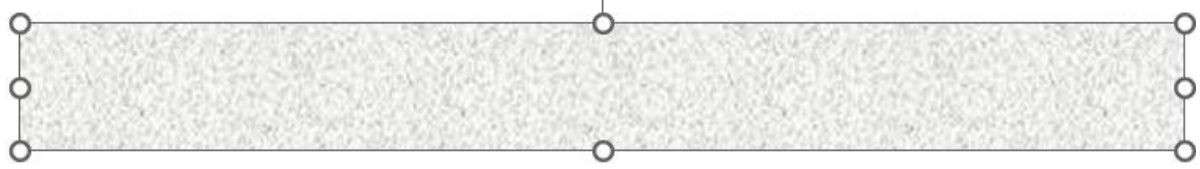
Implementing shatter-resistant film on glass doors is a cost-effective solution that strengthens the glass surface, making it significantly more difficult to break. This delays or deters forced entry attempts, reducing the risk of unauthorized access, theft, or vandalism. Although replacing glass doors with solid-core or reinforced materials requires a higher initial investment, it provides long-term security benefits by eliminating visibility into restricted areas and preventing intruders from targeting valuable IT equipment. These measures enhance privacy, improve overall security resilience, and reduce potential financial losses from stolen assets or security breaches.

Follow-Up Actions:

- Fit shatter-resistant film on all glass doors within 1 month; plan replacement with solid-core doors in the next quarter.
- Reinforce door locks where needed; phase out weaker locking mechanisms.
- Perform a physical security risk assessment after installation of films and new locks.
- Update maintenance and inspection routines to include checks of door integrity and security film condition.

References

Alamsyah, R. and Arifin, Y., 2024. 'Integrated Framework for IT Asset Physical Security: A Risk Management Approach Using NIST and ISO Standards'. *2024 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia, 2024, pp. 405-411. doi:<https://doi.org/10.1109/ICITSI65188.2024.10929290>



Appendix A: Work-In-Progress Notes

1. Initial Report – Planning and Preparations

Date: 10th March 2025

Task Details:

The initial task involved reviewing all provided documents, including the client's letter, ISO27002:2022 section 7, and the audit specification. This was essential for understanding the audit's scope and the constraints imposed.

Decision/Approach:

The audit focused on physical security controls within the [REDACTED] Building labs, specifically secure areas and equipment security. No interaction with university staff or students was permitted, requiring the audit to be conducted from a student's perspective. Observations were to be made regarding visible security measures such as access control and equipment siting.

Rationale:

By thoroughly understanding the client's constraints and requirements, the audit could be executed without raising suspicion or disrupting [REDACTED] operations, ensuring adherence to ethical guidelines. This approach was also intended to maintain the audit within the defined scope while promoting a good relationship with the client.

Key Actions:

- Review of all provided documentation.
- Development of an understanding of the audit scope.
- Formulation of the audit strategy within the provided constraints (e.g., no staff interaction and a student-like perspective).

2. Intermediate Report – On-Site Observations & Preliminary Findings

Date: 15th March 2025

Task Details:

At this stage, the focus was on checking how secure the entrances to the labs were and how the equipment inside was protected. This involved looking at locks, keypads, and other entry control systems, as well as checking the placement of equipment to make sure it was safe from damage and unauthorized access.

Decision/Approach:

The audit looked at how people can enter the secure areas, such as through locked doors, badge readers, or keypads. The effectiveness of these controls was noted. Additionally, the equipment inside the labs, like computers and cables, was checked to ensure it was placed safely to avoid damage from things like electrical problems or fire, and to make sure it couldn't be easily stolen or tampered with.

Rationale:

Physical access control is essential for securing sensitive areas, such as computing labs, by preventing unauthorized entry. By observing the access control systems, the audit aimed to identify potential security gaps that could go unnoticed. Effective access control and proper equipment protection are crucial to ensuring the safety of both the lab environment and the equipment inside. This stage helped to identify

weaknesses in the security measures and provided a foundation for recommendations to improve the lab's overall security and meet the required standards.

Key Actions:

- Checked how doors and entry systems work like locks, badge readers, keypads.
- Looked for any problems like unlocked doors or weak entry controls.
- Reviewed where equipment was placed to make sure it wasn't at risk from things like electrical surges or being damaged.
- Checked that cables and devices like computers were securely placed to reduce the chance of unauthorized access or tampering.

3. Final Report – Analysis and Audit Completion

Date: 22nd March 2025

Task Details:

The final stage involved analysing the findings from the on-site observations and reviewing the effectiveness of physical security controls within the computing labs. This included assessing the security of the access points, the overall lab perimeter, and the protection of sensitive equipment. Key findings from earlier observations were now consolidated to identify security gaps and provide actionable recommendations.

Decision/Approach:

The analysis focused on determining whether the existing security measures were adequate to meet the lab's security requirements, specifically in terms of controlling access and safeguarding equipment. The approach was to identify areas where security could be improved, considering the observed weaknesses in entry controls and equipment protection. The findings were then used to propose solutions that would enhance security without causing unnecessary disruption.

Rationale:

Proper security controls are crucial to safeguarding sensitive information and equipment. The analysis aimed to ensure that the lab's physical security measures were aligned with best practices, as outlined in ISO27002:2022. By identifying weaknesses, the goal was to improve security measures and recommend changes that would better protect the labs from unauthorized access or environmental threats. The findings helped to ensure the lab met the necessary security standards and provided a foundation for ongoing improvements.

Key Actions:

- **Reviewed the Effectiveness of Access Controls:** Focused on the strengths and weaknesses of door locks, keypads, and badge readers to determine their ability to prevent unauthorized entry. Examined the security of emergency exits, windows, and other potential entry points to ensure they were properly secured.
- **Consolidated Findings on Equipment Protection:** Evaluated whether equipment was adequately protected from environmental risks and whether cables were properly secured to avoid tampering or accidental damage.
- **Identified Areas for Improvement:** Noted areas where access control could be strengthened such as better lock systems or clearer signage and where equipment could be more securely protected like improving cable protection.

Appendix B: Security Checklist

1. Secure Areas

Control Area	Checks	Notes / Findings
Physical Security Perimeter	Verify presence of walls, gates, and reception areas around secure facilities.	The computer lab is enclosed within sturdy building walls, with secured doors and windows.
	Inspect for physical barriers preventing unauthorized access to sensitive areas.	Wooden doors are present at the entrance of the lab.
	Check if external areas are well-lit to deter unauthorized access (e.g., working lights around entrances and walkways).	The entrance and surrounding areas are well-lit.
	Ensure external doors and windows are properly secured (e.g., functional locks, self-closing doors, secured windows).	Functional locks and self-closing doors are in place. Windows are secure but lack locks.
Physical Entry Controls	Ensure that entry points are equipped with access controls such as locks, card readers, or biometric scanners.	No multi-factor authentication (MFA) such as biometrics or card swipe was present.
	Ensure emergency exits are secured against unauthorized access but remain accessible for safety.	Emergency exits are well-secured, with fire action plans and fire extinguishers in accessible locations and in good condition.
Securing Offices, Rooms, and Facilities	Ensure there are visible security signs (e.g., "Restricted Area", "CCTV in Operation") at key entry points.	CCTV covers lab areas and entry points.
	Inspect locks, security systems, and doors for physical protection of rooms and offices.	All locks and doors are in good condition with no signs of wear and tear.
	Ensure offices containing sensitive equipment are locked when not in use.	Data room and penetration testing lab were locked, requiring proper authorization for access.
Working in Secure Areas	Check that guidelines for working in secure areas are available and followed by personnel.	Posters and guidelines were displayed, covering updates, system unplugging procedures, and CCTV monitoring policies.
	Ensure proper protection procedures are in place when working with sensitive data or equipment.	No sensitive data was exposed; staff and students were cautious about protecting personal information.

2. Equipment Security

Control Area	Checks	Notes / Findings
Equipment Siting and Protection	Confirm that all equipment is sited in secure locations to minimize theft or damage risks.	Computing resources were found in open-access labs, with no clear separation from surrounding areas
	Ensure that system placement prevents unauthorized viewing of sensitive information.	Workstations were placed too close together, increasing the risk of shoulder surfing
	Ensure that unused or non-functional equipment is properly stored in designated areas.	A portable air conditioner with an "Out of Order" sign was observed in an open lab area
	Check that computers and IT assets are physically secured to desks (e.g., cable locks).	In the second-floor labs, systems such as CPUs and desktops were securely embedded into desks and locked, but in the lower floor labs, systems including CPUs and monitors were unsecured to desks
Supporting Utilities	Inspect the equipment for backup power (e.g., UPS) to prevent power failures.	No visible UPS backup—unknown if present.
	Check for adequate environmental controls (e.g., cooling systems, proper ventilation) in computing areas.	Ceiling ventilation systems, poster on windows to keep windows open and windows blinds were present.
Cabling Security	Inspect cabling for physical protection against damage or tampering.	All cables were in good condition, with no visible damage.
	Ensure critical infrastructure cabling is secured.	The electrical riser cupboard, which contains critical cabling and electrical infrastructure, was securely locked,
	Check that network and power cables are organized and protected from damage.	In some areas, cables were entangled, creating obstructions and increasing wear and tear risks and in other areas, network and power cables were properly routed through structured cabling systems
	Check that unused IT cables are stored securely	Unused cables were stored in an open cupboard near the lab entrance, which could be a security risk.

Appendix C: Photographic Evidence

Photographic evidence is provided in this appendix to support the claims and observations discussed in the report. These images offer visual confirmation of the findings and provide further context to the analysis.

1. Secure Areas



Figure 1 Building entrance security check



Figure 2 Lab Entrance Door



Figure 3 Vulnerable Glass Door in Computing Lab



Figure 4 Data room secured access via pin/card entry

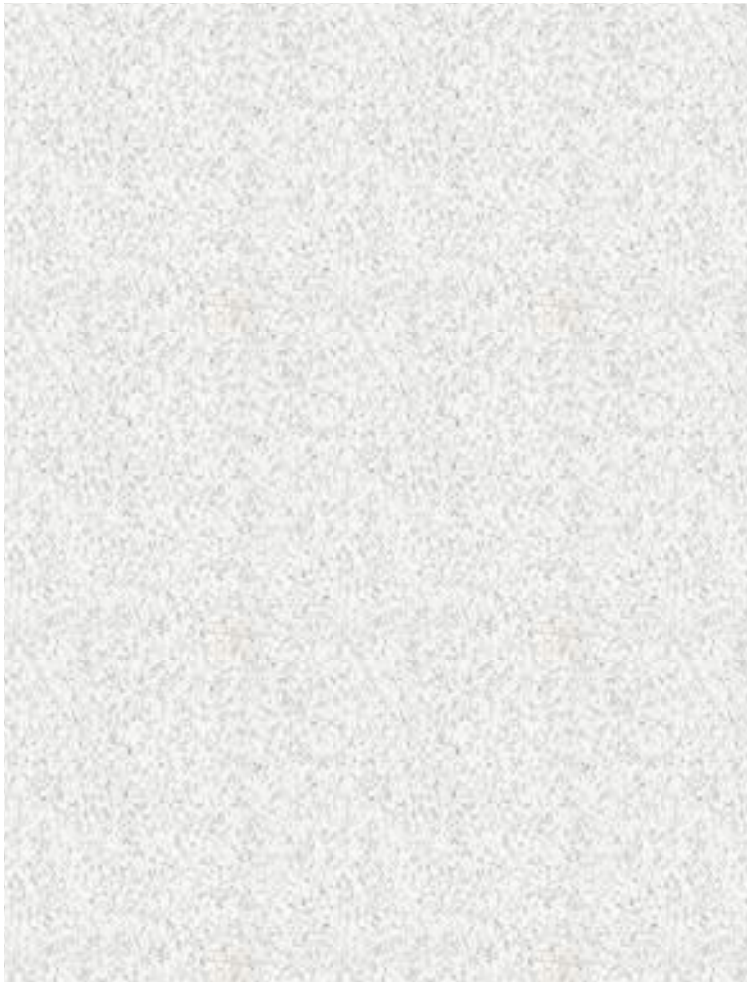


Figure 5 Electrical Riser area Secured and locked



Figure 6 Security awareness Posters

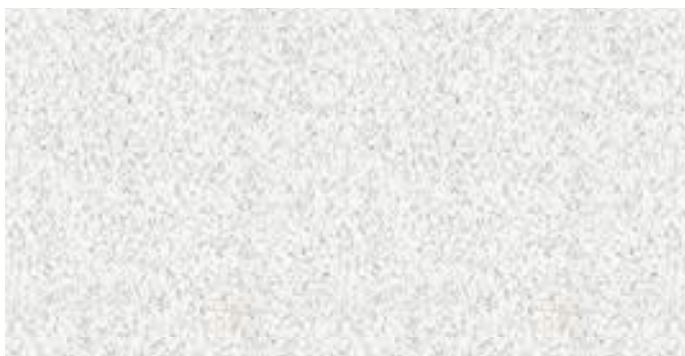


Figure 7 Security awareness Posters 2



Figure 8 Fire action plan

2. Equipment Security



Figure 9 System securely mounted



Figure 10 Systems unmounted from desk



Figure 11 Systems Placed Too Close, Leading to Shoulder Surfing



Figure 12 Non-Functional Portable Air cooler



Figure 13 Unused IT Cables Loosely Stored



Figure 14 Extension boards and cable trays



Figure 15 Ventilation Poster and Blinds on Window



Figure 16 Entangled Cables Creating Obstructions and Wear, leading to security and safety risk