This report is a team product, reviewed through regular work-in-progress meetings, and its content integrated and jointly agreed by all authors. It represents a true statement of the team's audit findings and conclusion.

Audit Report of "Stockwell Street Facility of University of Greenwich" according to *ISO 27002:2022*

CyberSAFE

Date: 22nd March, 2024

Priyank Raval – 001337526

This CyberSAFE Audit Report is addressed to
L. Clancy, Manager at Manager CMS Support.

Table of Contents

Section 1: Scope

The overall objective of this audit is to evaluating the physical controls and equipment security measures implemented within Library and Studio rooms of the University of Greenwich facility located at Stockwell Street in Greenwich. This audit report adheres to the specifications outlined in the letter by the manager of CMS support at the University of Greenwich and aligns with Section 7 of ISO 27002:2022, emphasizing the importance of physical controls and equipment security.

The audit will cover the following Sections from ISO 27002:2022:

- 7.1 - Physical security perimeter
- 7.2 - Physical entry controls
- 7.3 - Securing offices, rooms and Facilities
- 7.6 - Working in secure areas
- 7.8 - Equipment siting and protection
- 7.11- Supporting utilities
- 7.12 - Cabling Security

This auditor does not visit staff rooms, seminar rooms, or utility areas, as specified in deliverables and only audit from a point of view perceptive without any conversation with the member of the university staff. Additionally, sections of ISO27002:2022 that are not relevant to this audit, such as Clear Desk/Screen Policy, Assets Off-Premises, Storage Media, Equipment Maintenance, Disposal/Reuse of Equipment, and Protecting Against External and Environmental Threats, will be excluded from the scope.

Section 2: Business Setting

The Stockwell Street building consists of four floors including basement, situated in London, United Kingdom, serves as the University of Greenwich's library facility. Within this building, there are Group Study rooms, individual glass pods, and a silent zone, catering to the diverse study needs of students, faculty, and researchers. This building also consists a lecture theatre which is crucial in facilitating the university's teaching and learning facility across different fields of study. The library offers access to a laptop, desktop computers, internet services, wide array of academic resources, including books and journals and printing area at each floor.

The Stockwell Street Facility ensures security through various physical measures. These include security guard stationed at the entrance, requiring ID cards for entry, staffs are available to assist students. A visitor register is maintained to track, and a staff member is responsible to provide tours of building and escort visitors to the entrance. Fire alarm systems are in place to alert occupants in case of emergencies.

Some threats to physical and equipment security have been identified, such as students being able to remove laptops from the building without being detected by staff or security guards. Additionally, group study rooms are not soundproof, resulting in audio leakage to neighbouring rooms, which can disrupt meetings or interviews involving students or staff.

Section 3: Practical Audit Method Employed

To assess the compliance of the Stockwell Street facility's information regulations, procedures, and protocols with Section 7 of ISO 27002:2022, we systematically reviewed them through the following procedures.

1. **Observation:**
   - The team conducted observations of the facility's information handling procedures by reviewing guidelines on-site and observing various notices and policies in action. This was done to identify any potential gaps from established procedures.
2. **Check Lists**
   - We created a checklist (See Appendix B) aligned with the Physical Security Measures & Equipment Security in the ISO 27002:2022 guidelines. This checklist was followed throughout the auditing process, serving as a systematic approach to assess and ensure compliance with the specified security standards and protocols.
3. **Testing**
   - We tested the effectiveness of current controls and procedures manually without disturbing staff members. We documented our findings to evaluate how well the existing measures are working.
4. **Fieldwork**
   - During our fieldwork, we adhered to our checklist to test the effectiveness of controls in accordance with compliance standards. We observed the implementation of procedure to access whether they were being followed correctly. we took photographs of various areas within the premises as evidence to support our findings and documentation process.

Section 4: Secure Areas

4(a). Expected Controls

ISO 27002:7.1 Physical Security Perimeter

- Defining a physical perimeter of Stockwell Street facility at University of Greenwich that is used to protect areas containing information about an organization and its assets.
- Establish robust fencing, walls, ceilings, and flooring around Stockwell Street facility to prevent unauthorized access.
- Ensure that doors and windows are securely locked when not in use, and implement external protection measures for windows and ventilation points to enhance security.
- Install CCTV cameras to monitor the perimeter and important areas, ensuring they cover blind spots and provide clear visibility day and night. Assign security personnel to monitor the camera feeds.
- To identify unauthorized entry attempts and notify security personnel, it is advisable to install motion detectors and alarms along the secured perimeters.

ISO 27002:7.2 Physical Entry Controls

- Restrict the access of Stockwell Street to authorized personal only.
- Use systems such as electronic card readers, biometric scanners (fingerprint, retina scans), or PIN-based systems to allow entry to only authorized personnel.
- Implement electronic card readers, biometric scanners (fingerprint or retina scans), or PIN-based systems to permit entry solely for authorized personnel.
- Establish a reception area at the entrance with a security guard to oversee physical activity. Also, secure emergency exists points from unauthorized access.
- Develop and enforce procedures for managing visitors, including issuing temporary passes, escorting visitors while on premises, and ensuring visitors are properly identified and authorized.
- Inspect incoming deliveries for illegal materials like explosives, chemicals, or hazardous substances before moving them to the loading section.

ISO 27002:7.3 Securing Offices, Rooms and Facilities

- Create group study rooms, offices, and meeting rooms that prevent outsiders from seeing or hearing confidential information or activities.
- Keep internal telephone directories and online maps of confidential information processing facilities restricted from unauthorized access.
- Place directional symbols, warning signs, or caution notices on private areas, and limit entry to authorized individuals using their biometric or ID cards.

ISO 27002:7.6 Working in Secure Areas

- Only disclose details of assets or activities within a secure area (For verification, please refer to Appendix C) on a need-to-know basis, and restrict access to individuals authorized to work in that area.
- Prohibit the use of photographic, video, audio, or other recording equipment in secure areas unless authorized.
- Ensure proper control over the handling and use of user endpoint devices within secure areas.

4(b). Observed Controls and Comments

ISO 27002:7.1 Physical Security Perimeter

Observed Controls:

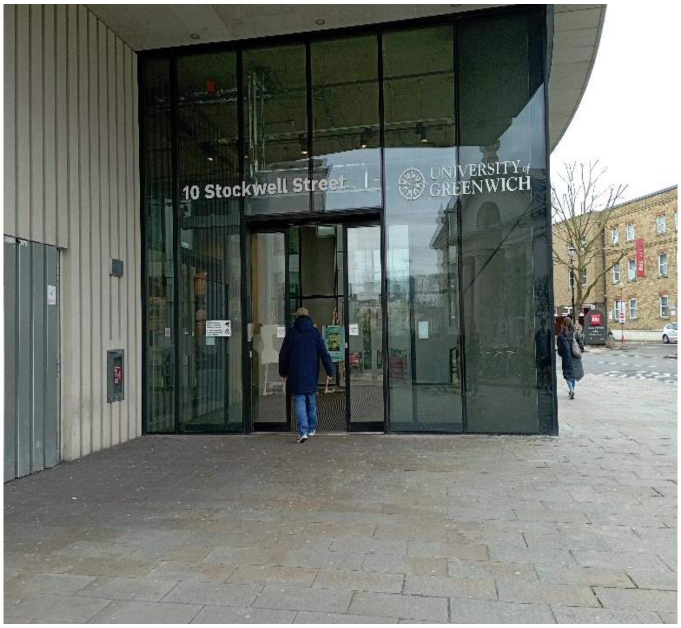


Figure 1: Main Entry into Stockwell Street Facility

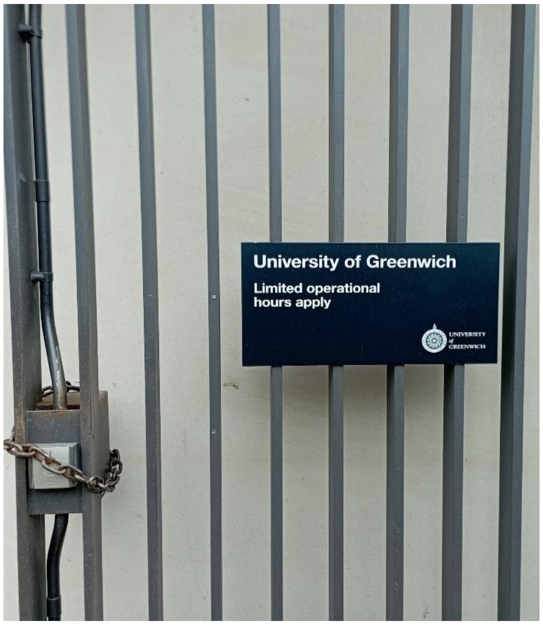


Figure 2: Physical Perimeter gate besides the buildings

- **As seen in Figure 1**, We observed the main entry of the Stockwell Street facility which is equipped with an automatic door that operates using sensors, allowing it to open upon the arrival of a person.

- Next to Stockwell Street, there is a narrow road leading towards the University of Greenwich campus as in **Figure 2**. This door is only open in Business hours and also Information label is placed on the door describing owner of the area and warning regarding operational hours.

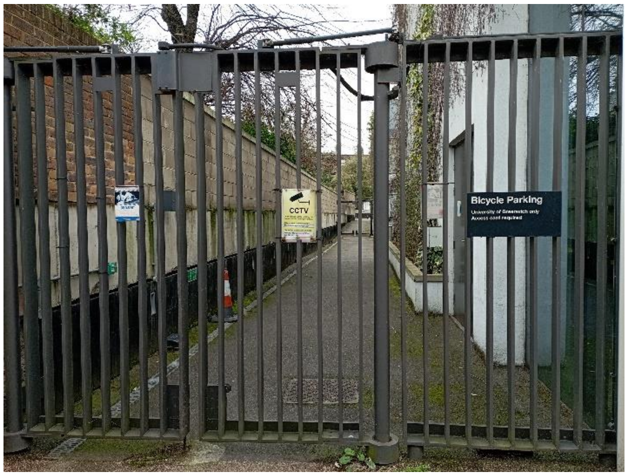


Figure 3: Rear area with bicycle parking facilities.

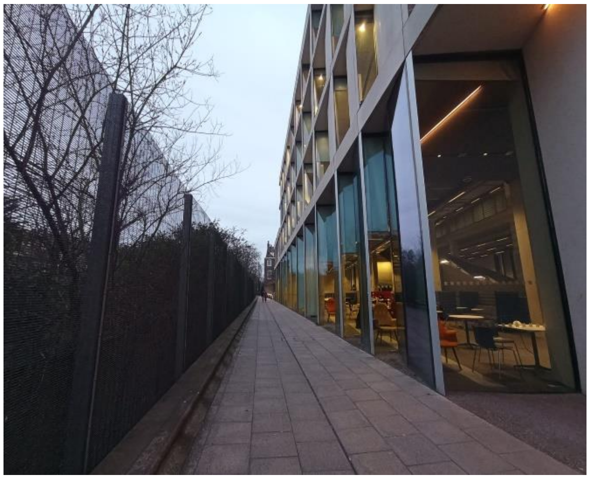


Figure 4: Exterior View: The Premises' Wall

- we checked out the back area of the building shown in **Figure 3**. There are two entrances, both monitored by cameras. Access through gate requires an electronic card, ensuring only authorized people get in.
- Majority of the wall at Stockwell Street facility is constructed with glass panels, as depicted in **Figure 4**. Surrounding the premises is wired fencing, and rear section is enclosed by brick walls.

Comments:

- Cameras are only installed in the rear areas of the premises; otherwise, we did not observe any cameras in other exterior locations around the premises.
- The premise's wall is not up to standard because it's made of glass. The usual recommendation is to use concrete or cement, which is much harder to break.

ISO 27002:7.2 Physical Entry Controls

Observed Controls:

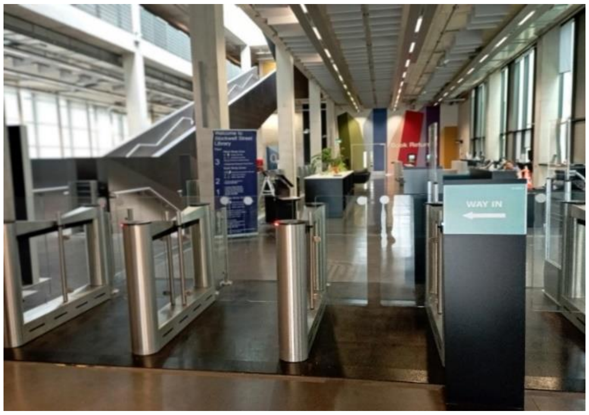


Figure 5: Entry barrier with electronic card reader

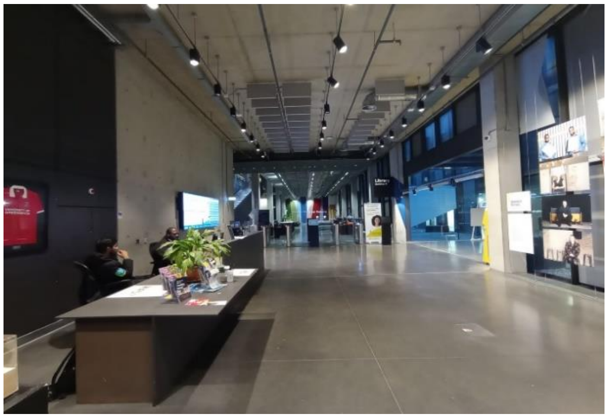


Figure 6: Security Desk near entry barriers

- Access to the premises is securely controlled by barrier that only opens with an authorized electronic card, complying with standard security protocols as seen in **Figure 5.**
- Security personnel are stationed at the security desk, situated close to the entry barriers, to ensure thorough monitoring of the premises and individuals who enter in this premises.
- When individuals arrive to visit the premises without an ID card or authorized entry, security guard records their name, contact information, purpose of visit, and the time of arrival etc., in the visitor log book kept at the security desk.

Comments:

- During our visit, we observed instances during our visit where students were exchanging ID cards with others to gain entry into the premises. This behavior poses a serious threat to the security of the facility. We suggest training security personnel to detect and address this behavior.
- There is no visitor badge policy in place, making it difficult to distinguish between authorized personnel and visitors, which poses a security risk within the premises.

ISO 27002:7.3 Securing Offices, Rooms and Facilities

Observed Controls:

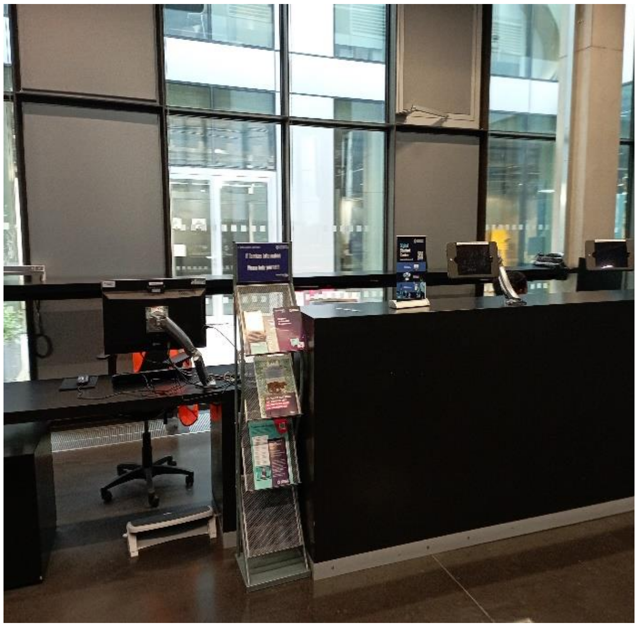


Figure 7: Reception desk

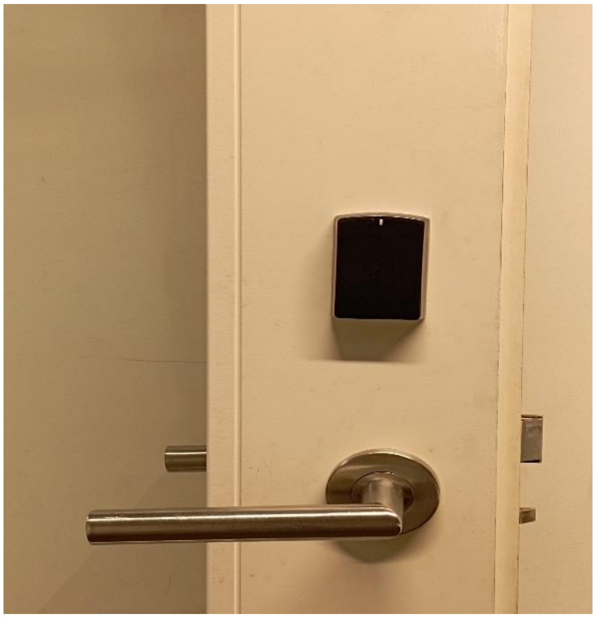


Figure 8: Card reader in Group Study room

- A reception area is situated on the ground floor as seen in **Figure 7**, to assist students, staff, and other individuals with their queries and concerns. The administration at this desk is responsible for approving requests for group study rooms.

- The facility has group study rooms for meetings and collaborative work, situated in various zones within the premises. Access to these rooms is restricted to authorized individuals who must book the group study room in advance before accessing it. As seen in **Figure 8** card reader is available for accessing it.

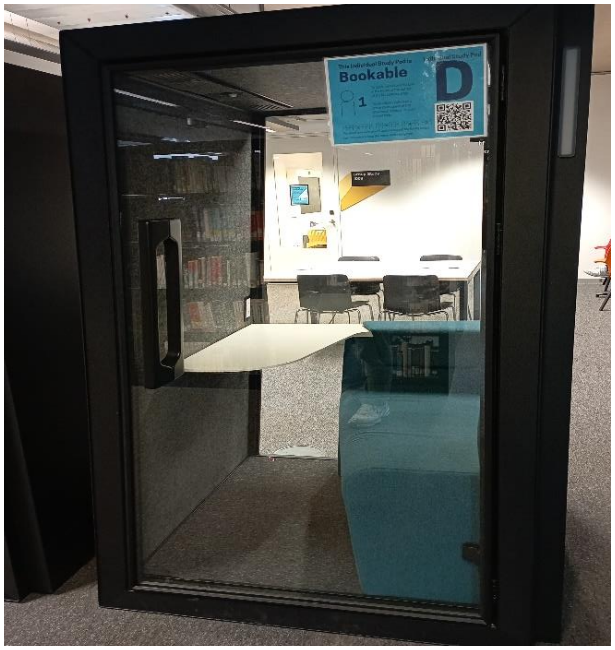


Figure 9: Individual Glass Pod

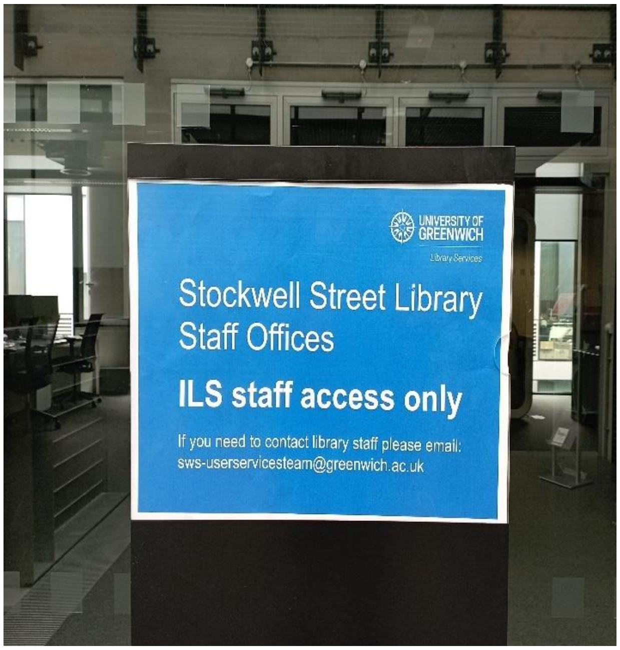


Figure 10: Warning sign

- Individual glass pods are provided for individuals as seen in **Figure 9,** seeking a quiet space for interviews or personal work. These pods feature soundproof glass to ensure privacy and minimal disruption.
- To ensure the security of staff offices within the premises, we see a signboard, as depicted in **Figure 10**, is prominently displayed. This sign clearly states that only staff members are permitted access and provides contact details in case of emergencies.

Comments:

- During our initial meeting, we noticed that noise from neighboring rooms was audible, indicating that the group rooms are not soundproof.
- The premises lack security cameras, creating blind spots and making it difficult to monitor individuals effectively. According to ISO 27002:2022, installing cameras covering all areas is recommended.

ISO 27002:7.6 Working in Secure Areas

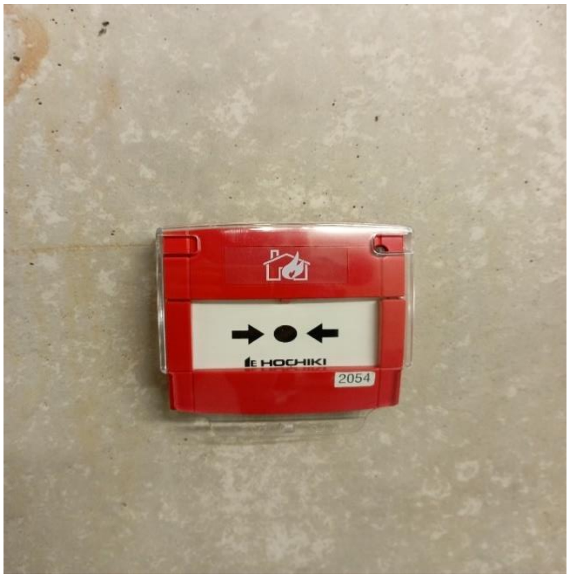


Figure 11: Fire alarm switch

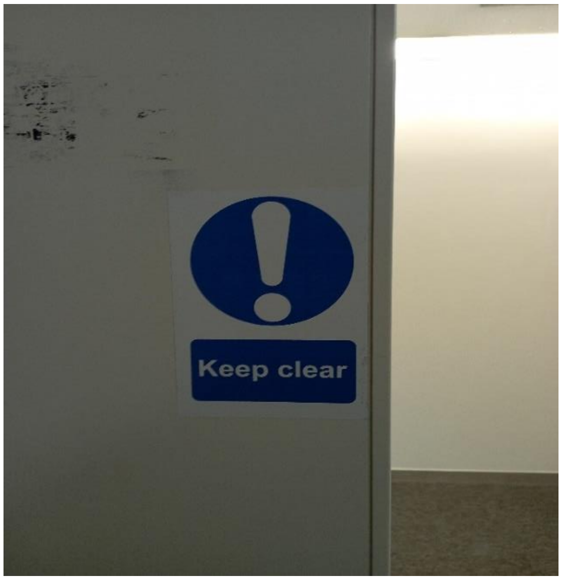
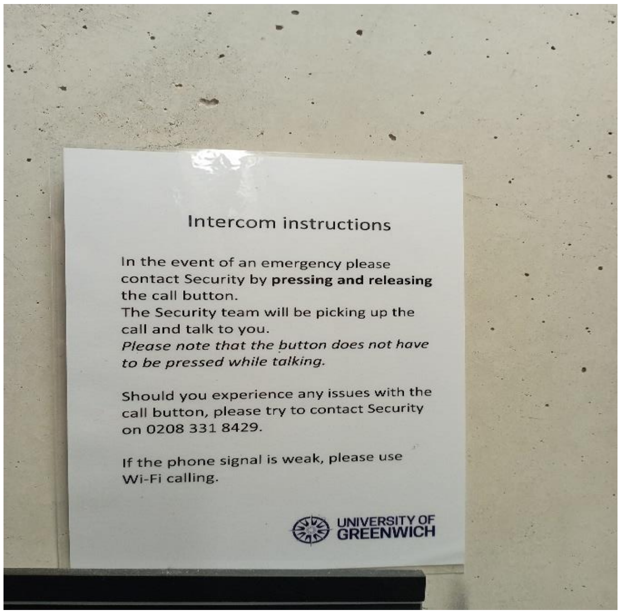


Figure 12: Simple Instruction

Observed Controls:

- We noticed that the fire alarm system is installed throughout the premises, as shown in **Figure 11**. This is a crucial safety measure for the people working in the facility and for the overall security of the organization.
- We observed that on every exit door, there is an emergency signboard with the instruction "Keep Clear" as seen in **Figure 12**. This serves as a reminder for everyone to ensure that no objects or hazards obstruct these areas in case of an emergency.



Intercom instructions

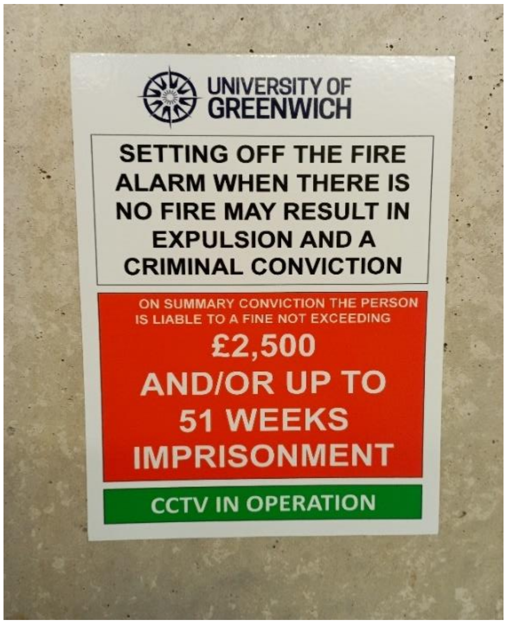
In the event of an emergency please contact Security by **pressing and releasing** the call button.
The Security team will be picking up the call and talk to you.
Please note that the button does not have to be pressed while talking.

Should you experience any issues with the call button, please try to contact Security on 0208 331 8429.

If the phone signal is weak, please use Wi-Fi calling.

UNIVERSITY OF GREENWICH

Figure 13: Intercom Communication in Emergency



UNIVERSITY OF GREENWICH

SETTING OFF THE FIRE ALARM WHEN THERE IS NO FIRE MAY RESULT IN EXPULSION AND A CRIMINAL CONVICTION

ON SUMMARY CONVICTION THE PERSON IS LIABLE TO A FINE NOT EXCEEDING
£2,500
AND/OR UP TO
51 WEEKS
IMPRISONMENT

CCTV IN OPERATION

Figure 14: Warning for misusing Fire Alarm.

- We noticed that intercom communication systems are in place for emergency situations as seen in **Figure 13**, and there are clear instructions provided on how to use them, especially in the absence of network connectivity or call button is not working.
- Additionally, warnings about the consequences of misusing the fire alarm system are prominently displayed in red color as seen in **Figure 14**. This ensures that individuals are aware of the seriousness of false alarms and discourages any unauthorized activation, preventing unnecessary panic or evacuation.

Comments:

- We noticed that there are no restrictions on taking photographs or videos within the premises, which could pose a potential threat to the organization's security. Therefore, it is recommended to implement a policy regarding the use of recording devices to mitigate this risk.

Section 5: Equipment Security

5(a). Expected Controls

ISO 27002:7.8 Equipment Siting and Protection

- Set up guidelines for eating, drinking and smoking (Refer Appendix in premises near equipment and critical assets.
- Implement controls to minimize the risk of various physical and environmental threats, like theft, fire, water damage, and vandalism.
- Keep electronic device such as laptops in locker and only accessible through ID card.
- Implement a device management system and assign a unique Device ID to every piece of equipment utilized within the facility.
- Secure the excess wiring of peripherals such as the mouse, keyboard, and other devices connected to the PC using small cable ties to bundle them together.

ISO 27002:7.11 Supporting Utilities

- Regularly inspect and test equipment utilized to support utilities like water supply, telecommunication, electricity, ventilation, and air conditioning to guarantee they operate effectively.
- Guarantee that the building's utilities can operate smoothly without interruption, and ensure there are sufficient resources available to accommodate growth and interaction with other utilities.
- Establish alarms to promptly identify malfunctions in utilities, such as fire alarms, water leakage alarms, and provide emergency contacts for addressing such malfunctions, including overflow emergencies.

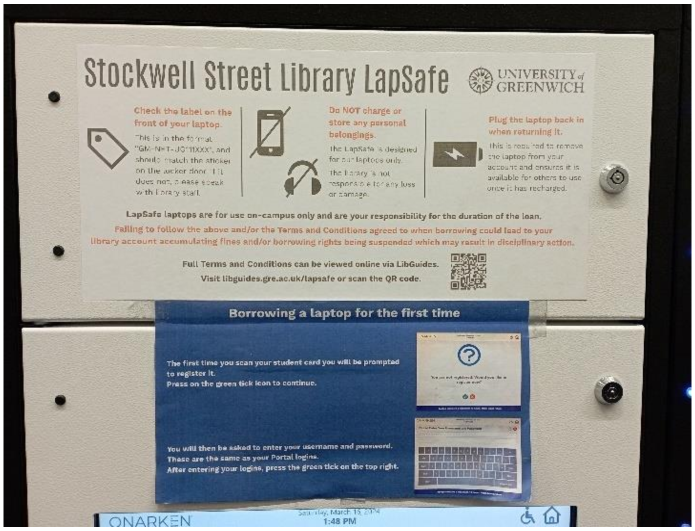
ISO 27002:7.12 Cabling Security

- Whenever possible, install power and telecommunication lines underground. When located outside, ensure adequate alternative protection such as cable protectors is in place. Additionally, to prevent wire cuts, utilize Armored Conduit.
- To prevent interference, segregate power and communication cables for sensitive and critical systems.
- Conduct regular technical sweeps and physical inspections to detect any unauthorized devices attached to cables.
- Label cables at both ends to facilitate easy physical identification during cable inspection.

5(b). Observed Controls and Comments

ISO 27002:7.8 Equipment Siting and Protection

Observed Controls:



Stockwell Street Library LapSafe

UNIVERSITY of GREENWICH

Check the label on the front of your laptop. This is in the format "GM-NFT-JG11XXX", and should match the sticker on the locker door. If it does not, please speak with library staff.

Do NOT charge or store any personal belongings. The LapSafe is designed for our laptops only. The library is not responsible for any loss or damage.

Plug the laptop back in when returning it. This is required to remove the laptop from your account and ensures it is available for others to use once it has recharged.

LapSafe laptops are for use on-campus only and are your responsibility for the duration of the loan.

Failing to follow the above and/or the Terms and Conditions agreed to when borrowing could lead to your library account accumulating fines and/or borrowing rights being suspended which may result in disciplinary action.

Full Terms and Conditions can be viewed online via LibGuides. Visit libguides.gre.ac.uk/lapsafe or scan the QR code.

Borrowing a laptop for the first time

The first time you scan your student card you will be prompted to register it. Press on the green tick icon to continue.

You will then be asked to enter your username and password. These are the same as your Portal logins. After entering your logins, press the green tick on the top right.

Figure 15: Instruction for borrowing Laptop

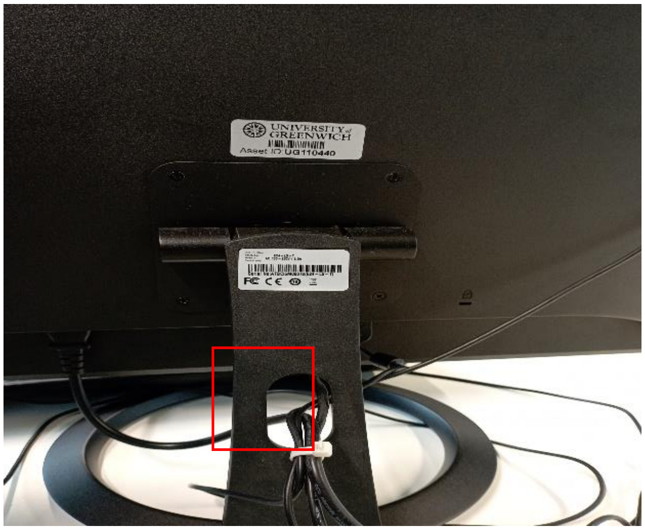


Figure 16: Protected mouse and Key board

- We observed that when borrowing a laptop, students or staff must scan their ID card, and it is mandatory to return it by 10:00 PM daily. All of these instructions and guidelines are provided, as seen in **Figure 15,** which is very helpful for borrowers.
- We observed that to secure the mouse and keyboards, small cable ties are used to bundle the excess, with cable ties as seen in **Figure 16** to securing them.

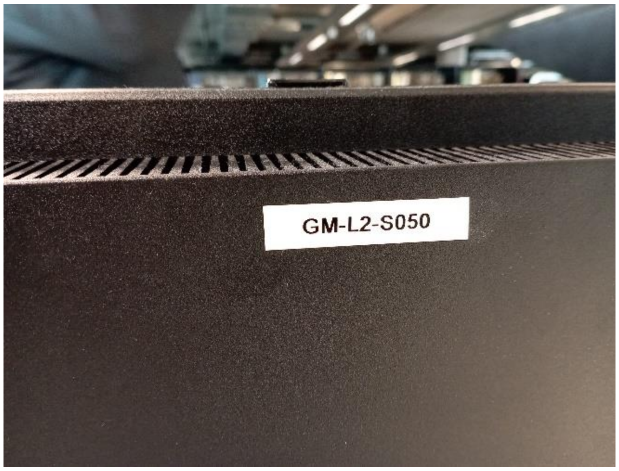
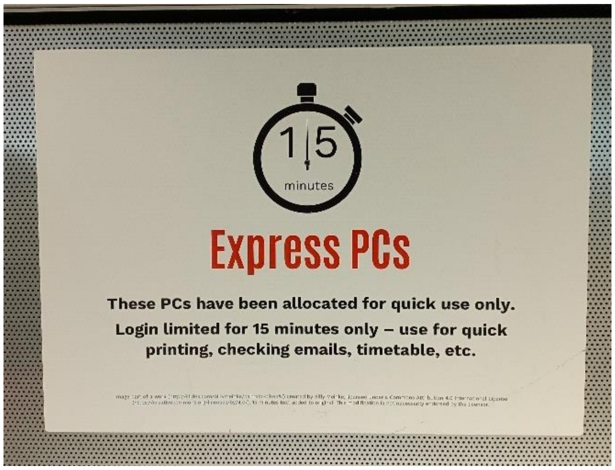


Figure 17: Asset Identity Number



Express PCs

These PCs have been allocated for quick use only.
Login limited for 15 minutes only – use for quick printing, checking emails, timetable, etc.

Figure 18: Instruction for Printer Machines

- We noticed that the organization has assigned asset identification numbers, as shown in **Figure 17**, according to standards. This practice facilitates easy identification of assets in case of issues, which is a commendable security measure.

- For utilizing printing service and PC, notice is displayed as seen in **Figure 18**. It mentions PCs are only logged in for a max of 15 minutes for quick printing to prevent long queues.

Comments:

- We observed that some students take laptops outside of the premises without notifying staff or security personnel. This poses a risk of laptops being stolen from the premises.
- We have also observed instances where students remove the mouse and keyboard wires to use them with their own laptops. Additionally, some students bring their own devices and occupy Facility PCs, preventing others in need from using the machines.

ISO 27002:7.11 Supporting Utilities

Observed Controls:

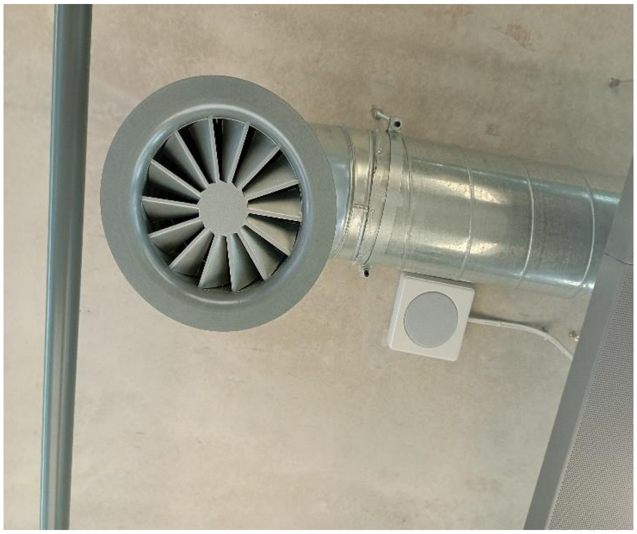


Figure 19: Ventilation

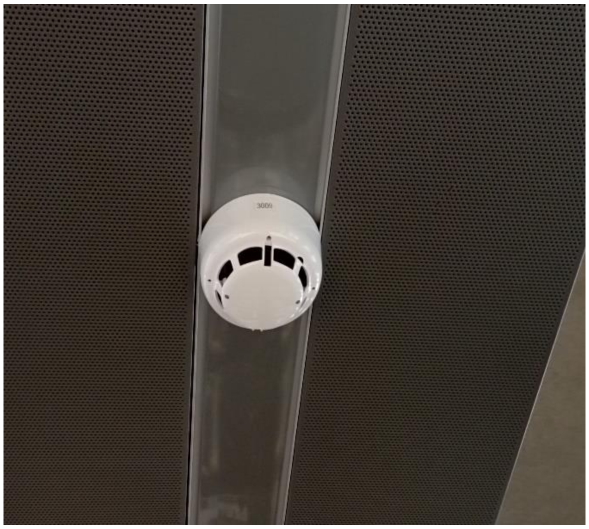


Figure 20: Smoke Detection Alarm

- **Figure 19** illustrates the presence of ventilation throughout the facility, which helps reduce heat generated by desktops and laptops and keeps the premises cool and comfortable. Also, lowers humidity levels and removes airborne pollutants, ensuring a cleaner and more comfortable atmosphere.
- **Figure 20** shows smoke detection systems installed throughout the facility. They quickly detect fires, sound alarms for emergencies, and help evacuate the premises while alerting the administration for necessary actions.

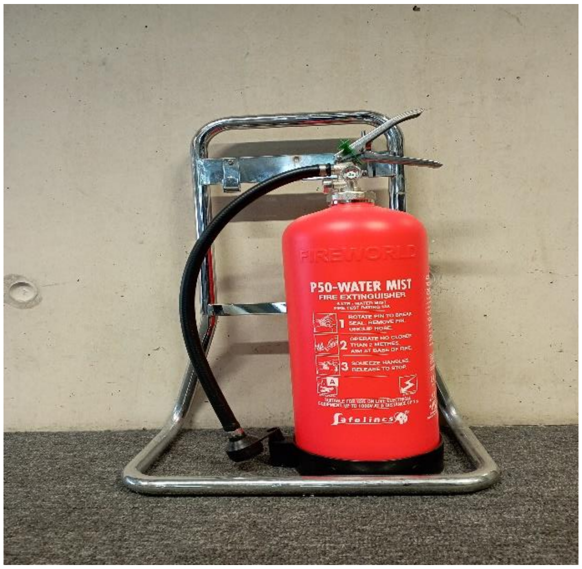


Figure 21: Fire Extinguisher

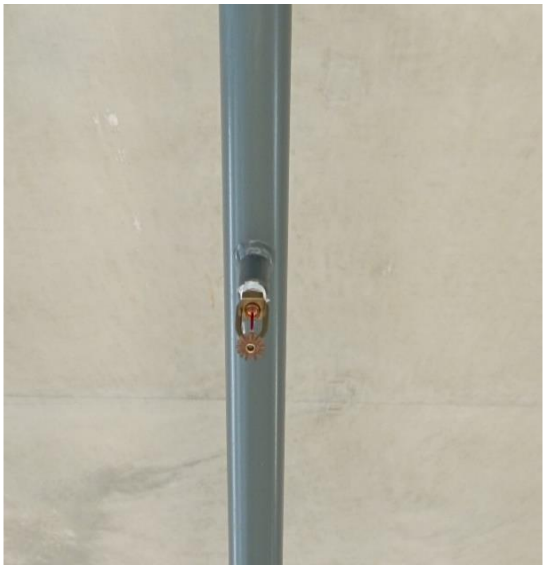


Figure 22: Fire Sprinkler

- Fire extinguishers, depicted in **Figure 21**, and fire sprinklers, shown in **Figure 22**, are installed throughout the facility to assist in case of a fire emergency.
- Periodically, the administration team conducts fire drills to ensure all equipment is functioning properly and individuals are familiar with the procedure.

Comments:

- We observed that the facility is equipped with appropriate preventive measures in case of disasters such as fire.
- We have also observed Emergency Fire Exit doors available on each floor, with maps of assembly area locations placed beside each fire exit door, which we designate as "Fire Action." Please see the Appendix C for more informative images.

ISO 27002:7.12 Cabling Security

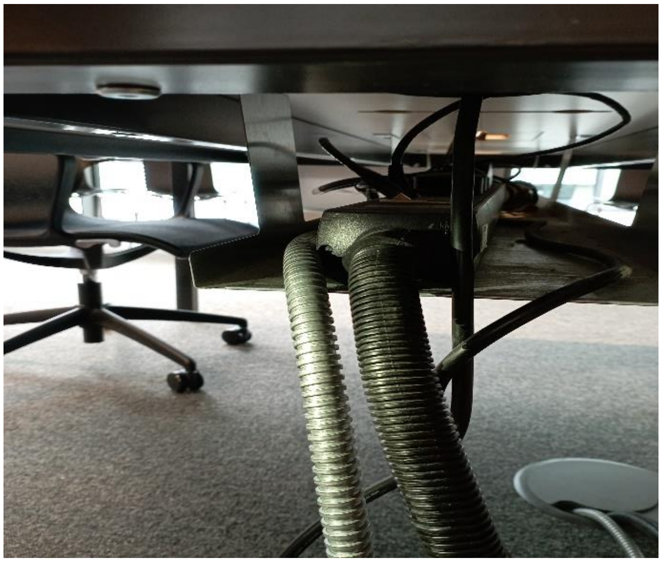


Figure 23:Seperated & Secure Power and Internet Wire

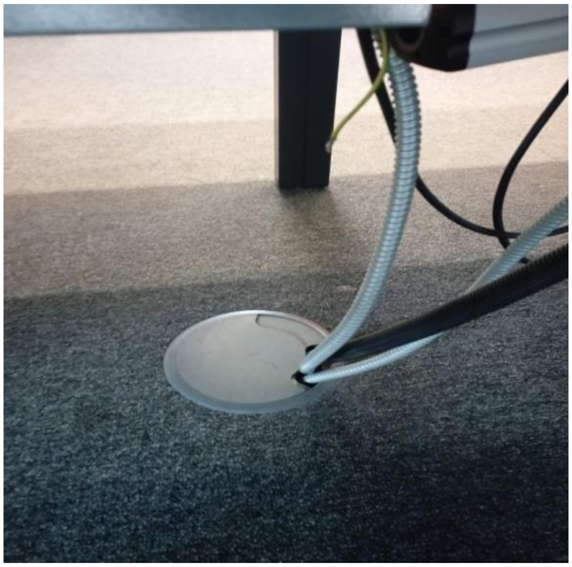


Figure 24: Underground Cables

- In **Figure 23,** We observed that power cables and internet cables are segregated using two distinct cable protectors. Armored conduit is utilized to safeguard fiber and ethernet cables from potential cuts or damage.
- As depicted in **Figure 24**, all internet and power cables are installed underground to mitigate risks associated with higher voltage lines. Underground wiring not only provides increased reliability but also enhances security compared to overhead lines.

Comments

- Our observation and analysis indicate that the organization has effectively implemented cable security measures by securely placing them underground in accordance with ISO 27002:2002 standards. No further action is deemed necessary for cable security.

Section 6: Audit Conclusion

6(a) Overall Conclusion Based on Relevant GAP Analyses

ISO27002:2022 Information Security Controls Section 7: Physical Controls	Efficient Standard Implementation 75-100%	Future enhancements 25-75%	Immediate Implements are required 0-25%	Comments
Are Physical Security Permitter were Defined?	100			In Compliance according to ISO 27002:2022 s7.1.
Are the walls constructed using robust materials like bricks?		45		Walls should construct using strong materials rather than glass.
Does CCTV cameras in place?			15	CCTV cameras has to be installed inside the premises.
Is motion detector being in place to identify unauthorized entry?		35		In future motion detector needs to be implemented to detect unauthorized entry.
Does ID card, pin or biometric scanners are present for authorized entry?	100			In Compliance according to ISO 27002:2022 s7.2.
Is there physical security guard present at the entrance?		65		Security guards present, but students can enter using another student's ID card so training required for guard.
Are visitor log books available?	100			In Compliance according to ISO 27002:2022 s7.2.
Are visitor badges available for entry into the premises?			25	Visitor badges are not provided to visitors at the Stockwell Street facility.
Is the soundproofing equipment installed in the meeting rooms?		40		Occasionally, noise from neighboring rooms can be heard in other rooms.
Are there any emergency action plans, notices, or warnings in place for private areas?	100			In Compliance according to ISO 27002:2022 s7.3.
Is internal confidential information handled securely?	100			In Compliance according to ISO 27002:2022 s7.3.

Are premises only accessible by authorized personnel?	100			In Compliance according to ISO 27002:2022 s7.6.
Is the use of photographic or other recording equipment prohibited in secure areas?			25	We noticed individuals taking many pictures, including in restricted areas.
Are there adequate controls and policies in place for the use of user endpoint devices?	100			In Compliance according to ISO 27002:2022 s7.6.
Are there any prohibitions against eating, drinking, and smoking?	100			In Compliance according to ISO 27002:2022 s7.8.
Are there measures in place to reduce risks from theft, water damage, fire, and vandalism?	100			In Compliance according to ISO 27002:2022 s7.8.
Are electronic devices such as laptops and desktop PCs accessible only to authorized personnel?	100			In Compliance according to ISO 27002:2022 s7.8.
Are there security measures in place to prevent laptop theft?		45		We observed incidents where some students were able to take laptops outside the premises.
Are excess wires of devices such as mice and keyboards secured with cable ties?	100			In Compliance according to ISO 27002:2022 s7.8.
Are regular inspections in place for supporting utilities such as ventilation, water supply, etc.?	100			In Compliance according to ISO 27002:2022 s7.8.
Is the facility equipped to handle fire incidents with fire alarms and sprinkler systems in place?	100			In Compliance according to ISO 27002:2022 s7.8.
Can the facility address malfunctions in daily-use services like toilets, water supply, or sewage blockages?		50		We encountered issues with toilets being occasionally blocked and unavailable for use.
Are the cables used for internet and power segregated and installed underground?	100			In Compliance according to ISO 27002:2022 s7.12.
	1400	280	65	
Compliance = (1745/2300) * 100% = 75% compliant. So, the GAP is 100% - 75% = 25%.				

6(b) Recommendation for Immediate and Future Management Action

- Constructed a sturdy wall using cement blocks and bricks, opting for durable materials that are challenging to penetrate.
- We've identified multiple blind spots within the premises, so it is recommended to installing security cameras as soon as possible to cover these areas. This will help protect and monitor against any suspicious activity on the premises.
- Enforce a policy requiring all students to wear ID cards during lab time and implement verified badges for visitors, students, and staff.
- We observed that some students can enter in to premises with some other student id card so train security personal to suspect this behavior and take strict action against such individuals.
- Introduce temporary and restricted access permissions for the secure area.
- We've noted instances where students are able to remove laptops from the facility without being noticed by security personnel, resulting in thefts. It's recommended to install an alarm system or incorporate a tracking chip into laptops. This way, if someone attempts to take a laptop outside, an alarm will sound, alerting security.
- Construct soundproof group study rooms, as we've observed that noise from neighboring rooms can significantly disrupt initial audit meetings held within these spaces.
- Enforce a policy prohibiting the use of photographic, video, audio, or any other recording equipment in secure areas unless expressly authorized.

References

Aquino, C. (2023) ISO 27002-2022.PDF, SlideShare. Available at: https://www.slideshare.net/ChristianAquino52/iso-270022022pdf (Accessed: 02 March 2024).

Group, E. (2022) The new ISO 27002, Blog. Available at: https://www.eraneos-ch.blog/blog/the-new-iso-27002 (Accessed: 02 March 2024).

NQA Gap Analysis, NQA. Available at: https://www.nqa.com/en-gb/certification/gap-analysis (Accessed: 02 March 2024).

Appendix A: Minutes of Work-in-Progress Meetings (Initial, Interim, Final)

Initial Meetings:

We decided to meet in person to review the documents provided by Robert Beadle, the Chief Auditor at CyberSAFE Auditors. The documents included the Audit Job Allocation directed towards Trainee Auditor Team from Robert Beadle, the original letter from client which specifies the scope and constraints to be followed while conducting the audit. The third document was a section from the ISO27002 which describes physical controls to prevent access and ways to secure equipment.

We thoroughly read and understood the documents and deliverables and decided the responsibilities of each team member and ensured that everyone understood their duties for the audit. We also discussed how to carry out the audit while following the constraints. Each member expressed their opinion, and all the points were noted down. We also walked around the library and studio rooms to make sure everyone understood the scope. There was a little conflict while deciding the timeline of the actions but eventually everyone agreed. We carefully assigned the tasks and planned out further steps. We also set up shared document which can be updated by each member, so all the information is at a single place.

Interim Meetings:

After wrapping up the audit using the methods outlined in our initial meeting, we proactively scheduled interim meetings to track progress. These sessions served as checkpoints to discuss the audit's advancement, ensuring alignment with our predetermined schedule and objectives. At these gatherings, we crafted a progress report card, detailing completed tasks and addressing any encountered challenges. Through open dialogue, we collectively devised solutions to overcome obstacles encountered during the audit process.

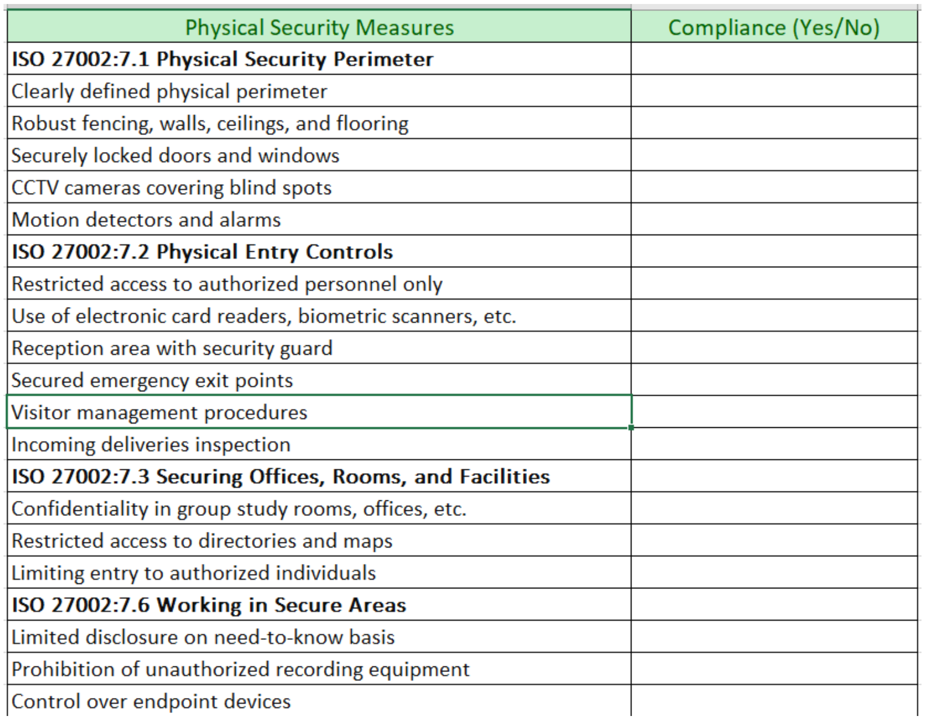
Furthermore, we updated all audit-related documentation, including reports, notes, and suggestions, with the aim of enhancing future processes. With these updates in place, we focused on comprehensive documentation, laying the groundwork for compiling the final report. During this phase, we deliberated on the structure and content of the final report, ensuring it encapsulated our findings, recommendations, and insights gleaned from the audit process. Our collaborative efforts during these meetings were instrumental in ensuring a thorough and effective audit outcome.

Final Meeting:

After completing our individual reports, we met in person to create the Final Report. Together, we proofread each other's documents and swiftly resolved any issues. We designed a header page and wrote a Joint Authorship Statement. We successfully created the report and Finally submitted it to L. Clancy, the Manager of CMS Support.

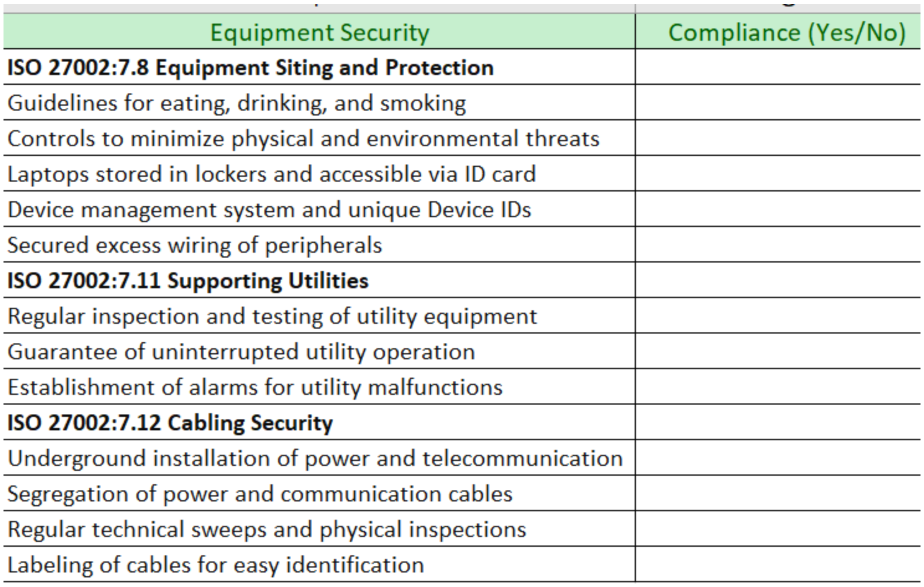
Appendix B: Checklist Template Created for Auditing

We have developed the following checklist as shown in below Figure, for conducting an audit of the Stockwell Street Facility in accordance with the guidelines outlined in ISO 27002:2022 Section 7.



Physical Security Measures	Compliance (Yes/No)
ISO 27002:7.1 Physical Security Perimeter	
Clearly defined physical perimeter	
Robust fencing, walls, ceilings, and flooring	
Securely locked doors and windows	
CCTV cameras covering blind spots	
Motion detectors and alarms	
ISO 27002:7.2 Physical Entry Controls	
Restricted access to authorized personnel only	
Use of electronic card readers, biometric scanners, etc.	
Reception area with security guard	
Secured emergency exit points	
Visitor management procedures	
Incoming deliveries inspection	
ISO 27002:7.3 Securing Offices, Rooms, and Facilities	
Confidentiality in group study rooms, offices, etc.	
Restricted access to directories and maps	
Limiting entry to authorized individuals	
ISO 27002:7.6 Working in Secure Areas	
Limited disclosure on need-to-know basis	
Prohibition of unauthorized recording equipment	
Control over endpoint devices	

Figure 25: Checklist for Physical Security Measures



Equipment Security	Compliance (Yes/No)
ISO 27002:7.8 Equipment Siting and Protection	
Guidelines for eating, drinking, and smoking	
Controls to minimize physical and environmental threats	
Laptops stored in lockers and accessible via ID card	
Device management system and unique Device IDs	
Secured excess wiring of peripherals	
ISO 27002:7.11 Supporting Utilities	
Regular inspection and testing of utility equipment	
Guarantee of uninterrupted utility operation	
Establishment of alarms for utility malfunctions	
ISO 27002:7.12 Cabling Security	
Underground installation of power and telecommunication	
Segregation of power and communication cables	
Regular technical sweeps and physical inspections	
Labeling of cables for easy identification	

Figure 26: Checklist for Equipment Security

Appendix C: Additional Security Controls are Currently Implemented

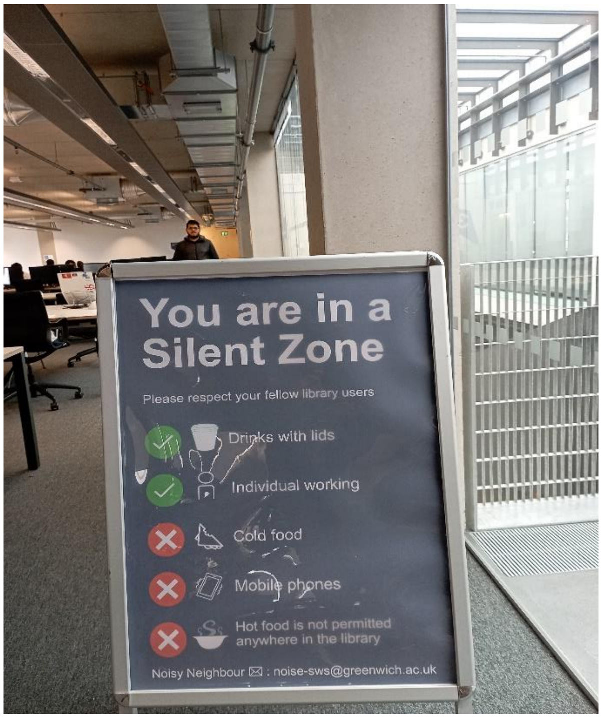

You are in a Silent Zone
Please respect your fellow library users
Drinks with lids
Individual working
Cold food
Mobile phones
Hot food is not permitted anywhere in the library
Noisy Neighbour ✉ : noise-sws@greenwich.ac.uk

Figure 27: Restriction on Food and Drink

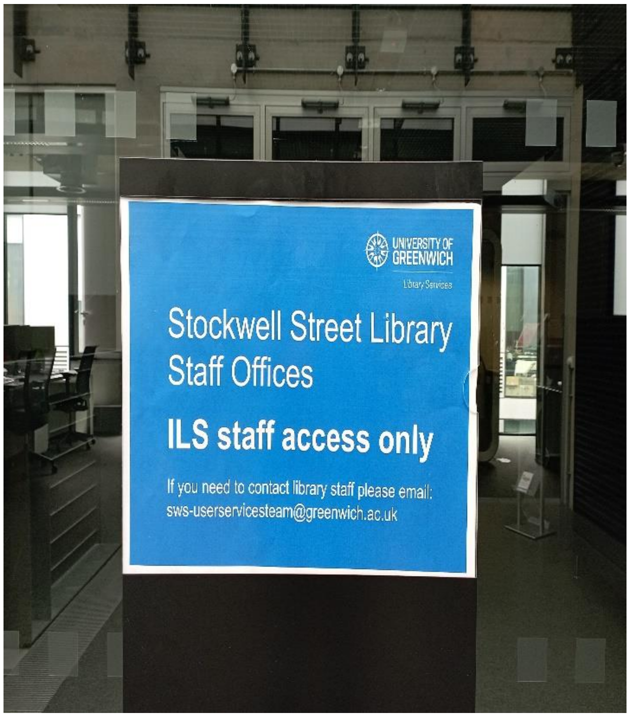


Figure 28: Warning of Restriction for authorized person only

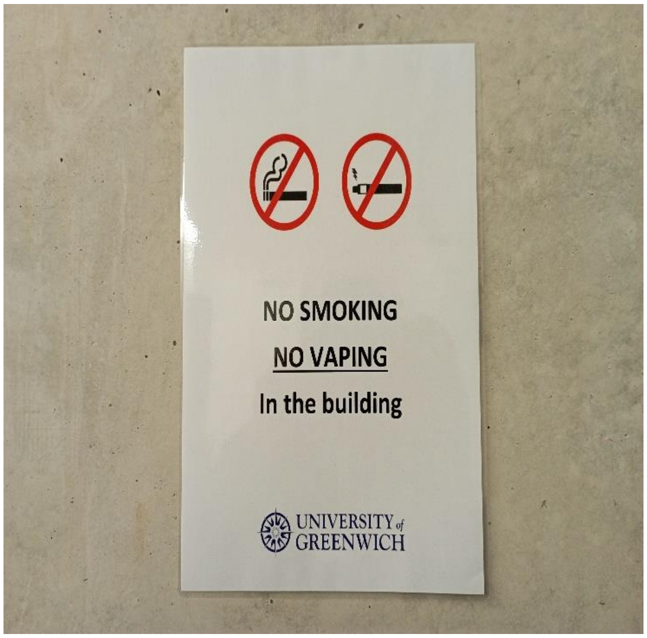


Figure 29: Smoking Restriction

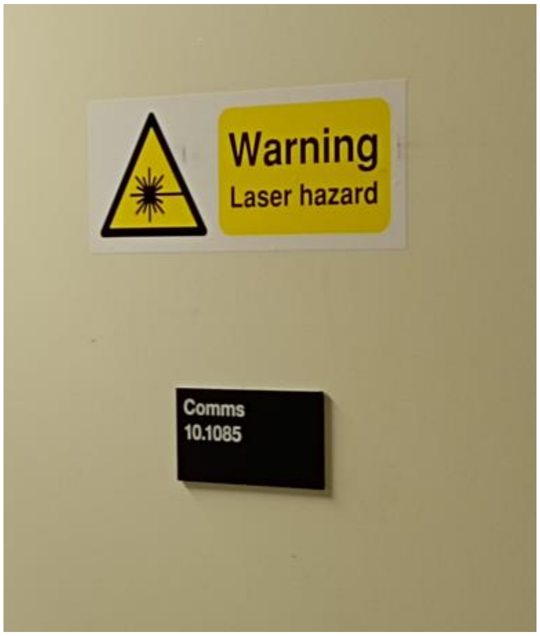
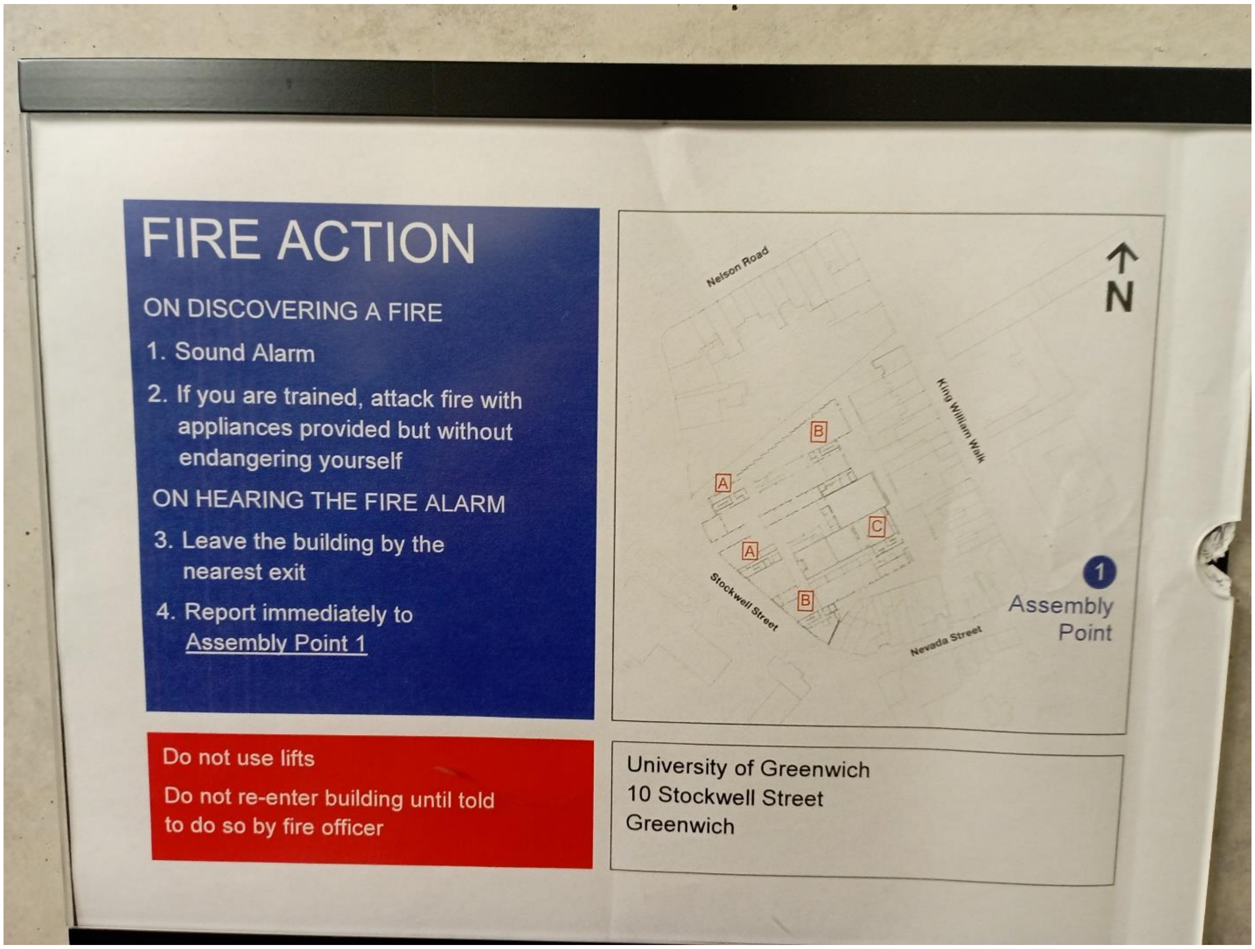


Figure 30: Warning sign for indivudul



FIRE ACTION

ON DISCOVERING A FIRE

1. Sound Alarm
2. If you are trained, attack fire with appliances provided but without endangering yourself

ON HEARING THE FIRE ALARM

3. Leave the building by the nearest exit
4. Report immediately to Assembly Point 1

Do not use lifts

Do not re-enter building until told to do so by fire officer

University of Greenwich
10 Stockwell Street
Greenwich

Figure 31: Emergency Fire Action Plan